FIPS PUB 201

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Federal
Personal Identity Verification (PIV)
Standard
DRAFT

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: Identification**

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

To be Issued February 25, 2005

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Philip J. Bond, Under Secretary

National Institute of Standards and Technology
Hratch G. Semerjian, Acting Director

NOTE FOR REVIEWERS

Please note that this is a preliminary draft of the FIPS. We're especially looking for general agreement/disagreement on high level design decisions to assist us in crafting the next draft of the FIPS. While we will consider all comments received in development of the next draft, we may not be able to respond directly to all comments.

Specific issues for which your inputs are most particularly desired include:

Image-based vs minutiae template-based biometric storage on the card
Match on card vs match off card biometric comparison
Specific mandatory card topology elements/placement/scale
Data model

We're working on the November 8 Formal Public Draft of FIPS 201, and early receipt of your views on these and other subjects that may be of particular interest to your Department or Agency will be essential to our revision efforts.

Please provide comments by 30 October, 2004. It is important to copy mehta_ketan@bah.com and grance@nist.gov on your comments.

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

XXXXXXXX, Director
Information Technology Laboratory

ABSTRACT

This standard specifies a framework, architecture, and technical requirements for a comprehensive federal personal identity verification system. The standard addresses several problems requiring reliable and cost effective solutions in personal identification as it applies to access control. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of an individual seeking physical access to various government facilities and electronic access to government information systems. The framework identifies the problems to be solved, defines a common identity verification architecture, and describes the components, interfaces, support services, and life-cycle management functions needed to achieve requisite levels of security assurance for applications that require different levels of protection.

Keywords: Architecture, authentication, authorization, biometrics, credential, cryptography, identification, identity, infrastructure, Federal Information Processing Standard (FIPS), framework, model, validation, verification.

Federal Information Processing Standards Publication 201

2005

Announcing the Federal
Personal Identity Verification
Standard

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. Name of Standard. Personal Identity Verification (PIV)

2. Category of Standard. Computer Security.

3. Explanation.

Homeland Security Presidential Directive (HSPD) 12, dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors", directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. It further specified secure and reliable identification that a) is issued based on sound criteria for verifying an individual employee's identity; b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; c) can be rapidly authenticated electronically; and d) is issued only by providers whose reliability has been established by an official accreditation process. Executive departments and agencies are required to use the standard for identifying Federal employees and contractors requesting access to Federally controlled facilities and logical access to Federally controlled information systems. Finally, the directive stipulates that the standard include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

This standard specifies a framework and technical requirements for a comprehensive federal personal identity verification system. The framework is designed to address and solve several problems requiring reliable and cost effective solutions in personal identification.. The overall goal is to achieve appropriate security assurance for applications by efficiently verifying and authenticating the claimed identity of an individual seeking physical access to various government facilities and electronic access to multiple government information systems. The framework identifies the problems to be solved, defines a common identity verification architecture, identity proofing through life cycle credentialing, and describes components, interfaces, support services, and life-cycle management functions needed to achieve requisite levels of security assurance for applications that require different levels of protection. The framework also incorporates and refers to other technical and operational standards necessary to achieve interoperability among identification cards, electronic card readers, communication systems, and access control systems interfaces.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

6. Applicability.

This standard is applicable to all Federal departments and agencies for verifying the identity of Federal employees or Federal contractors seeking physical access to Federal facilities or to sensitive information within Federal information systems that are not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code. This standard shall be used in designing, acquiring and implementing personal identity verification systems that Federal departments and agencies operate or which are operated for them under contract. This standard may be implemented on a voluntary basis by private and commercial organizations. This standard may be applied to other government affiliates, such as volunteers and students, by individual Federal agencies.

7. Specifications. Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) Standard (affixed).

8. Implementations.

The Personal Identity Verification standard specifies implementation and use of integrated circuit cards, often called smart cards, for use in a Federal personal identity verification system. The standard is designed to satisfy the requirements of HSPD-12 and to assure the interoperability of products and services developed in accordance with the standard.

Personal Identity Verification (PIV) cards must be personalized with identity information for the individual to whom the card is issued, for identity verification both by humans making visual comparisons between the cardholder and the information printed on the card and by automated systems electronically comparing identity information previously stored on the card and that supplied by the cardholder when requesting access. PIV cards contain one or more integrated computer chips to process identity verification requests using identity credential information stored within the ICC.

Graduated position sensitivity levels identified in the standard apply to identity source document proofing and authentication. The standard also covers card issuance and PIV operational system. NIST will develop a Personal Identity Verification Validation Program that will test implementations for conformance with this standard. Information on this program will be available at http://csrc.nist.gov/PIV-Project/Conformance/ as it becomes available.

9. Effective Date. This standard becomes effective February 25, 2005.

10. Qualifications.

The security afforded by the PIV system is dependent on many factors outside the scope of this

standard. Organizations adopting this standard must be aware that the overall security of the personal identification system relies on: 1) the assurance provided by the organization authorizing the creation and issuance of the PIV card that the person to be issued the credential has been correctly identified; 2) the position sensitivity levels selected by the PIV card issuer; 3) the protection provided to identity verification data stored within the PIV card and transmitted between the card and the PIV issuance system or access control systems; 4) the protection provided to the identity verification system throughout its entire life-cycle. Identity verification information (e.g., passwords, PIN's, personal cryptographic keys) provided by the individual must be protected against disclosure, duplication, and modification during the lifetime of the credential. While it is the intent of this standard to specify mechanisms and support systems that provide high assurance personal identity verification, conformance to this standard does not assure that a particular implementation is secure. It is the responsibility of the implementer to ensure that components, interfaces, communications, storage mediums, and services used within the identity verification system is designed and built in a secure manner.

Similarly, the use of a product containing an implementation that conforms to this standard does not guarantee the security of the overall system in which the product is used. The responsible authority in each agency shall assure that an overall system provides the acceptable level of security.

Since a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, this standard will be reviewed every five years to assess its adequacy.

11. Waivers.

As per the Federal Information Systems Management Act of 2002 (FISMA), waivers to Federal Information Processing Standards are no longer allowed. Organizations covered by the applicability section of the standard shall proceed to adopt and conform to the standard on a timely basis for their computer systems, information processing applications, and facilities.

12. Where to obtain copies.

This publication is available through the Internet by accessing http://csrc.nist.gov/publications/. A list of other available computer security publications, including ordering information, can be obtained from NIST Publications List 91, which is available at the same web site.

Federal Information Processing Standards Publication 201

Specifications for

Personal Identity Verification

TABLE OF CONTENTS

TABLE OF FIGURES

1. INTRODUCTION

Authentication of an individual's identity is a fundamental component of many physical and computer access control processes. When individuals attempt to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of identity provides a sound basis for such access control decisions.

A wide range of mechanisms are employed to authenticate identity, leveraging many different classes of identification credentials. For physical access, individual identity has traditionally been authenticated by use of paper credentials, such as driver's licenses and badges. Access to computers and data has traditionally been authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been applied to physical and computer security, replacing or supplementing the traditional credentials.

The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential. This document establishes a framework for Personal Identity Verification (PIV) credentials for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. These credentials are intended to authenticate individuals that require access to federal facilities, information systems, and applications. This framework addresses requirements for initial identity proofing, technical mechanisms for authentication for both physical and logical access, infrastructures to support interoperability of these mechanisms, and validation and accreditation of applications and processes implementing this specification.

1.1 Purpose

The purpose of this standard is to develop a reliable government-wide PIV system for use in applications of controlled access to federal facilities and information services. This standard has been developed within the context and constraints of federal policy and information processing technology currently available and evolving.

This standard establishes a framework for a PIV system within which cost effective and reliable identity credentials can be established and shared. The framework outlines a federal government-wide process for providing several levels of security depending on the risks to the facility or information being protected. The framework specifies an architecture, which constitutes a PIV system that can be provided by industry with currently available technology. Existing products or working models of components that satisfy the requirements and conform to the specifications are included in the architecture.

1.2 HSPD-12 Requirements

Homeland Security Presidential Directive 12 (HSPD-12), signed by the President in August 2004, established the requirements for a common identification standard for Federal employees and contractors. HSPD-12 directs the Department of Commerce to develop a Federal Information

Processing Standard (FIPS) defining secure and reliable forms of identification for issuance by the Federal Government to its employees and contractors. The standard is intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy.

HSPD-12 prescribes objectives, schedules, and features to be specified by this standard and identifies the organizations responsible for developing and adopting it. It does not specify the technologies, security mechanisms, and procedures to be used in accomplishing these objectives. According to the HSPD-12, the identification credentials shall be:

a) Issued based on sound criteria for verifying an individual employee's identity;
b) Resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
c) Rapidly authenticated electronically; and
d) Issued only by providers whose reliability has been established by an official accreditation process.

This standard establishes graduated criteria for physical and logical access credentials and identifies mechanisms for authentication of credential holders throughout the Federal Government. This standard also defines minimum technical and procedural requirements for the PIV system.

1.3 Problem(s) Being Addressed

NIST will address the requirements set forth in the HSPD-12 by developing a Personal Identity Verification (FIPS 201) standard that addresses the following threats:

- Cardholder makes improper use of a valid card
- Counterfeiting
- Stolen or borrowed cards are used to gain access
- Lower sensitivity cards are used to gain access to more sensitive and critical assets

2. GLOSSARY OF TERMS AND ACRONYMS

2.1 Glossary of Terms

The following definitions are used throughout this standard:

Application: A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system.

Access control: The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

Applicant: An individual requesting a PIV credential. The applicant may be a new Federal hire, Federal employee or contractor.

Approved: FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.

Architecture: A highly structured specification of an acceptable approach within a framework for solving a specific problem and containing descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable in order to satisfy related constraints (e.g., costs, local environment, user acceptability).

Asymmetric keys: Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Authentication: The process of establishing confidence in user identities.

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant.

Biometric Information: The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g. patterns.)

Biometric System: An automated system capable of:

- capturing a biometric sample from an end user;
- extracting biometric data from that sample;
- comparing the biometric data with that contained in one or more reference templates;
- deciding how well they match; and

- indicating whether or not an identification or verification of identity has been achieved.

Biometric Template: A characteristic of a biometric information (e.g. minutiae or patterns.)

Cardholder: An individual possessing an issued PIV card.

Capture: The method of taking a biometric sample from an end user. [INCITS/M1-040211]

Certificate Revocation List: A list of revoked public key certificates created and digitally signed by a Certification Authority. [RFC 3280]

Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

Certification Authority: A trusted entity that issues and revokes public key certificates.

Credential: An object that authoritatively binds an identity (and optionally, additional attributes) to and are controlled by an individual.

Comparison: The process of comparing a biometric with a previously stored reference template or templates. See also 'One-To-Many' and 'One-To-One' [INCITS/M1-040211]

Claimant: A party whose identity is to be verified using an authentication protocol.

Component: An element of a large system in general; specifically, an identity card, issuing authority, registration authority, Card reader, and identity verification support etc. within the personal identity verification system.

Conformance testing: a process established by NIST within its responsibilities of developing, promulgating, and supporting Federal Information Processing Standards for testing specific characteristics of components, products, and services as well as people and organizations for compliance with a FIPS standard.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

False acceptance: When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity. [INCITS/M1-040211]

False Acceptance Rate/FAR: The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as follows:
FAR = NFA / NIVA
where
FAR is the false acceptance rate

NFA is the number of false acceptances
NIVA is the number of impostor verification attempts
[INCITS/M1-040211]

False Match Rate/FMR: Alternative to 'False Acceptance Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'. See also 'False Non-Match Rate'. [INCITS/M1-040211]

False Non Match Rate/FNMR: Alternative to 'False Rejection Rate'. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an applicant. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'. See also 'False Match Rate'. [INCITS/M1-040211]

False rejection: When a biometric system fails to identify an applicant or fails to verify the legitimate claimed identity of an applicant. [INCITS/M1-040211]

False Rejection Rate/FRR: The probability that a biometric system will fail to identify an applicant, or verify the legitimate claimed identity of an applicant. The False Rejection Rate may be estimated as follows:
FRR = NFR / NEVA
where
FRR is the false rejection rate
NFR is the number of false rejections
NEVA is the number of applicant verification attempts
This estimate assumes that the applicant verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes 'Failure to Acquire' errors. [INCITS/M1-040211]

Federal Information Processing Standard (FIPS): A standard for adoption and use by federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce, covering some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Framework: A structured description of a topic of interest including: a detailed statement of the problem(s) to be solved and the goal(s) to be achieved; an annotated outline of all the issues that must be addressed while developing acceptable solutions to the problem(s); a description and analysis of the constraints that must be satisfied by an acceptable solutions; and detailed specifications of acceptable approaches for solving the problem(s) .

Graduated security: A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

Hash based message authentication code (HMAC): a message authentication code that uses a cryptographic key in conjunction with a hash function.

Hash function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:
1. (One-way) - It is computationally infeasible to find any input that maps to any pre-specified output, and
2. (Collision resistant) - It is computationally infeasible to find any two distinct inputs that map to the same output.

Identifier: A unique data string used as a key in the biometric system to name a person's *identity* and its associated attributes. An example of an *identifier* would be a Card number.

Identity: A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
.
Identification: the process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identity proofing: the process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registration Authority when attempting to establish an identity.

Identity registration: The process of making a person's *identity* known to the PIV system, associating a unique *identifier* with that identity, and collecting and recording the person's relevant attributes into the system.

Identity verification: the process of affirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information stored in the identity card or PIV system.

Interoperability: electrical, physical, logical, and structural compatibility among all the components, subsystems, and services of the PIV system assuring that an identity Card issued by one issuing agent may be verified by all verification subsystems at the requested level of assurance when all requested identity credentials are properly presented.

Match/matching: The process of comparing biometric information against a previously stored template(s) and scoring the level of similarity.

Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.

Model: a very detailed description or scaled representation of one component of a larger system that may be created, operated, and analyzed to predict actual operational characteristics of the final

produced component.

One-to-many: Synonym for 'Identification' [INCITS/M1-040211]

One-to-one: Synonym for 'Verification' [INCITS/M1-040211]

Online Certification Status Protocol (OCSP): An on-line protocol used to determine the status of a public key certificate. [RFC 2560]

Personal identification number (PIN): A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

Personal Identity Verification (PIV) Card: physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

PIV Requesting Official: An individual who can act on behalf of an agency to request a credential for an applicant.

PIV Authorizing Official: An individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant.

*PIV Issuance Authority: A*n authorized identity card creator that procures FIPS approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the card with the identity credentials of the authorized subject, and delivers the personalized card to the authorized subject along with appropriate instructions for protection and use.

PIV Registration Authority: An entity that establishes and vouches for the identity of an applicant to a PIV Issuing Authority. The PIV RA authenticates the applicant's identity by checking identity source documents and identity proofing and ensures a proper background check has been completed before the credential is issued.

Population: The set of end-users for the application. [INCITS/M1-040211]

Public Key: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Infrastructure (PKI): A support service to the PIV system that provides cryptographic keys needed to verify digital signature based identity verification and to protect communications and storage of sensitive verification system data within identity Cards and the verification system.

Registration: See Identity Registration

Recommendation: A special publication of the Information Technology Laboratory stipulating specific characteristics of technology to use or procedures to follow in order to achieve a common level of quality or level of interoperability.

Reference implementation: An implementation of a FIPS or a recommendation available from NIST/ITL for demonstrating proof of concept, implementation methods, technology utilization, and operational feasibility.

Secret key: A cryptographic key that must be protected from unauthorized disclosure in order to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.

Sensitivity levels: A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted.

Standard: A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.

Template: A biometric image data record. [INCITS/M1-040211]

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]

Verification: See Identity Verification.

2.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

AID Application Identifier

ANSI American National Standards Institute

ATR Answer-to-Reset

CAD Card Accepting Device

FID File ID

FIPS Federal Information Processing Standard

FIPS PUB FIPS Publication

GSC	Government Smart Card, as defined in the Smart Access Common Identification Card Solicitation.
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OCF	Open Card Framework
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
RFU	Reserved for Future Use
ST	Status Tuple
TLV	Tag-Length-Value

3. PIV OBJECTIVES

The FIPS 201 standard applies to all Federal departments and agencies that are currently responsible for issuing identity badges. Moreover, the standard applies to all personnel (i.e., Federal employees and contractors) who are already required by the Federal government to have an identity badge. The standard may be required by Federal departments and agencies to extend to other Federally controlled facilities, Federally controlled information systems, and Federal applications that are important for security and for which use of the standard in circumstances not covered by this directive should be considered. This standard establishes common objectives of the PIV system that apply across Federal departments and agencies.

3.1 Functional Objectives

The objectives of the PIV system are to:

- Collect and evaluate information sufficient to assure that the legal identity claimed by a PIV applicant is authentic;
- Provide an identity card to the applicant (now the PIV system subscriber) which may subsequently be used to verify this identity rapidly and securely;
- Specify interfaces necessary to read the identity card efficiently whenever offered by the cardholder when requesting access;
- Provide a method to verify that the cardholder is the claimed subscriber;
- Provide mechanisms that permit access control systems to determine that a claimed identity is correct;
- Provide appropriate security to the entire identity authentication and verification process commensurate with the desired level of security;
- Provide protection against use of cloned or counterfeited PIV cards;
- Provide adequate security technology, management procedures, and services to protect the PIV system from being circumvented;
- Support interoperability by allowing any subscriber holding a card from any issuer access to any authorized facility or information; and
- Protect the privacy of the subscriber.

3.2 Policy Objectives

The Personal Identity Verification (PIV) system shall be designed, implemented, and operated in a manner that assures accountability and privacy of the subscribers and availability, reliability, audit-ability, interoperability, security, and trust of the components comprising the system. This policy defines major objectives of the system and assigns responsibility for achieving these objectives.

Personal identity is the composite of certain characteristics of a human being, some which are unique (markers) and can be used as the basis for unambiguously recognizing that individual. Identification is recognizing the individual from a large number of individuals within some context. Identity authentication is the initial establishment of the legal name of the individual using

sufficient credentials that bind the claimed identity of a person with that person at a pre-determined level of assurance. Identity verification is subsequent comparison of a uniquely distinguishing characteristic (marker) of the individual with that previously captured from the authenticated person.

NIST is responsible for establishing standards, recommendations, guidelines, and conformance tests for components of the PIV system. Federal departments and agencies are responsible for adopting the NIST PIV documents and funding, procuring, and operating required PIV system components for their own employees and contractors. Each agency is responsible for: establishing sensitivity levels for positions; authenticating and vetting applicants for PIV cards; issuing PIV cards to approved applicants; authorizing PIV subscribers access to physical facilities and information systems; operating and maintaining their portion of the PIV system to assure the objectives of this policy; and cooperating with other agencies in using the PIV system to control and grant access to all people authorized at the level required by the facility or information system. DHS is responsible for reviewing and approving PIV sub-systems as meeting its directives; OMB is responsible for reviewing and approving PIV system budgets and operational procedures; GSA is responsible for assisting agencies to procure and operate PIV sub-systems; OPM is responsible for assisting agencies to authenticate and vet applicants in accordance with relevant laws and executive orders.

Specifically, applicants are responsible for providing authentic identity source documents when requested, completing accurately all position and PIV application forms, cooperating in the PIV applicant vetting process, and providing biometrics as needed; requesting officials are responsible for assuring that the position sensitivity level is appropriate and can be satisfied by the applicant; approving officials are responsible for assuring that all submitted information is appropriate and adequate for authenticating the identity of the applicant beyond a reasonable doubt; and PIV card issuers are responsible for matching the approved documents with the applicant and issuing a PIV card to the applicant (now PIV subscriber) with the requested and authorized personal and biometric data entered in accordance with PIV standards.

Specific policy directives and implementing instructions may be found in: FICC PIV policy documents; OMB PIV funding and operating directives; and GSA PIV procurement specifications.

4. PIV SYSTEM OVERVIEW

Identification of people seeking access (physical and logical) is a fundamental requirement for security. The primary goal of the PIV System is to achieve an appropriate level of authentication assurance by easily verifying the claimed identity of an individual seeking physical access to various government facilities and electronic access to multiple government services with confidence and in an interoperable manner.

The following sections discuss the PIV operational concept and various components that form the PIV System, its interactions as well as the lifecycle activities of the PIV Card.

4.1 Operational Concept

The PIV concept includes a process designed to assure issuance of electronic identity cards by only authorized issuers to only authorized recipients. This standard assures that the PIV cards are issued by agencies in a manner that meets consistent government-wide standards for the cards, the card issuance process, and the identity proofing of cardholders, so that cards will interoperate with access control systems across agencies and so that agencies can rely on cards issued by other agencies to make access control decisions. This standard does not set the access control policies of agencies.

The cards provide a suite of identity verification information and processes adequate to support verification of identity for access control use in a variety of Federal physical and logical access environments. Agencies and contractors issue PIV cards to their employees in a manner that conforms to the identity proofing and card issuance procedures of this standard. The mandatory features of the cards include a contact interface and a contactless proximity interface. The contactless interface allows readers to read a standardized digitally signed Cardholder Unique Identifier (CHUID) that includes the Federal Agency Smart Card Identifier Number (FACS-N). The contact interface allows the reader to access digitally signed cardholder biometrics information after the card has been unlocked by entering a PIN. The contact interface also allows the access control reader to read a cardholder authentication public key certificate and to perform a digital signature operation on challenges issued by the access control system, using the corresponding private key stored on the card. The certificate binds the common name of the cardholder, and the FACS-N to a public key, and is issued by a Certification Authority (CA), normally one of a few shared service provider CAs.

The authentication public key certificate can be used by agencies with suitable authentication protocols to authenticate the cardholder's identity and make access control decisions for physical access to facilities or logical access to information systems. The CHUID and biometrics are used only to make physical access control decisions.

There is no one comprehensive database of all issued cards nor are there public registries of cards that have been issued, however each issuing agency must retain records of the cards it issues. Similarly, CAs retain records of the certificates they issue, however do not make any public

registry of issued certificates available. The CHUID, biometric, and certificates contained on the card are authenticated by digital signature. However cards may be lost or may be revoked when cardholder status changes, and cards expire. Certificates are linked to the card (by the FASC-N), and must be revoked if the card is revoked. Each CA makes certificate revocation information publicly available on the Internet by publishing a Certificate Revocation List (CRL) and maintaining an On-line Certificate Status Protocol responder. Thus the revocation status of any card or certificate can be verified, however no database of issued cards or cardholder information is available.

4.2 Functional Components

This section provides an overview of the various functional components that comprise the complete PIV System. This system is logically divided into three major categories of components:

- **PIV System Front-End Components**: - consists of the PIV card, card and biometric readers, and the PIN Pad device. The PIV cardholder interacts with these components in order to gain physical or logical access to the desired federal resource.

- **PIV Card Issuance and Management Infrastructure Components**: - consists of the system components responsible for identity proofing and registration, card issuance and key management, as well as the various repositories and services (PKI credentials, card and certificate status servers etc) required as part of the verification infrastructure.

- **PIV Card Usage Infrastructure Components**: - consists of the physical and logical access control systems, the protected resources, and the authorization data.

The figure below illustrates the functional model for the PIV System, identifying the various system components and the direction of data flow between these components.

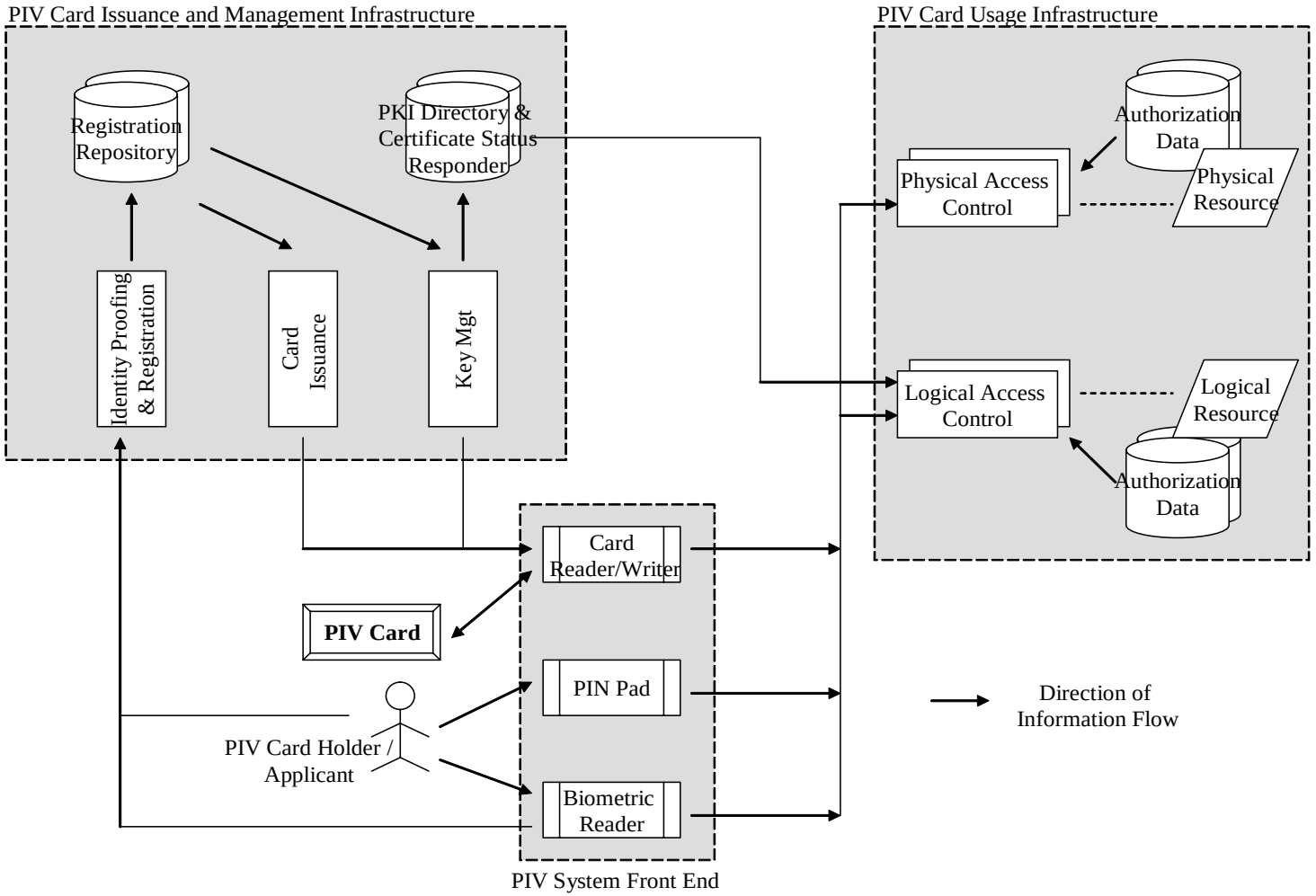


Figure 4-1: PIV System Functional Components

4.2.1 PIV System Front-End Components

The PIV card is issued to the applicant upon completion of all registration processes. This PIV card has a "credit card" sized form factor, with one or more embedded integrated circuit chips (ICC) that provide memory capacity as well as computational capability. This PIV card is the primary component of the PIV System and is used by its holder for authentication to various physical and logical resources.

Card readers are located at access points for controlled resources where a subscriber may wish to gain access (both physical and logical) by using the PIV card. The reader communicates with the PIV card to retrieve the appropriate information, located in the memory of the card, in order to pass it to the access control systems for granting or denying access.

Card writers are very similar to the card readers and are used for personalization and initialization of the information that needs to be stored on PIV cards. The data to be stored on these cards include personal information, certificates, the PIN, biometric data etc and is discussed in further detail in later sections.

Similar to the card reader, the biometric reader may be located at secure locations where a subscriber may wish to gain access by using the PIV card. It may be noted that while a card reader is essential to the use of a PIV card for electronic authentication, biometric readers are optional components that provide a higher level of assurance in the technical authentication of the cardholder. Biometric Readers depend upon the use of stored biometric templates of the cardholder, stored in the memory of the card, and it’s comparison of a real-time biometric sample to these stored templates. The use of biometrics provides an additional factor of authentication (something you are), in addition to providing the card (something you have).

As with a biometric reader, a PIN pad device can also be used along with the card readers at secure locations where a higher level of authentication assurance of the cardholder is required. The subscriber presenting the PIV card must type in their Personal Identification Number (PIN) into the PIN pad; the PIN pad then transmits the PIN either to the PIV card (for PIN comparison on the card) or to a backend control panel (for use of the PIN for authorization decisions.) The PIN pad therefore also supports the use of an additional factor of authentication (something you know), in addition to providing the card (something you have) to provide a higher level of authentication assurance.

4.2.2 PIV Card Issuance and Management Infrastructure Components

Identity Proofing and Registration deals with the collection, storage and maintenance of all information and documentation that is required to authenticate and assure the identity of the applicant. The goal of this step is to prove that the claimed identity of the Applicant is true (i.e. authentic) and that the set of identity source documents presented at the time of registration have been verified to be valid. Information such as the full name, address, date of birth, marital status, federal designation, sponsor identity, biometric information etc., are examples of information collected from the applicant at the time of registration.

The Registration Repository contains all the applicant registration data, collected at the onset of the registration process including the biometric data. Access to this repository is closely controlled with only authorized individuals allowed to read and/or modify contained information.

The PIV cards are capable of handling public key (PK) cryptography operations and can participate in PK enabled applications. The cryptographic keys held on a PIV card may be used in a challenge response protocol to verify the authenticity of the card as well as for providing data integrity and confidentiality through digital signatures and encryption. The generation of the key pairs, distribution of digital certificates containing the public key of the subscriber, management of the certificates so that application can be prohibited from using certificates which are no longer valid, are all part of Key Management component. This Key Management component is used throughout the lifecycle of PIV cards from issuance of PKI credentials to usage of PKI credentials for secure operations, to eventual re-issuance or termination of the card. It is also responsible for the provisioning of publicly accessible repositories and services (such as the PKI repository and the OCSP Responder Service) that inform the requesting application on the status of these PKI credentials.

The Card Issuance component primarily deals with the personalization of the physical (visual surface) and logical (contents of ICC) aspects of the card. This includes printing of photographs, name and other information on the card as well as loading the relevant card applications, biometrics and other relevant data onto it. The PIN to unlock the card is also collected (from the applicant) at the time of issuance, and embedded within the PIV card. In addition, this component is also responsible for providing status checks on the revocation status as well as the maintenance of each issued PIV card and the non-cryptographic data that is contained within it.

4.2.3 PIV Card Usage Infrastructure Components

Physical and logical resources are the end targets of the entire PIV system. A physical resource is the desired secured facility (building entrances, rooms, bathrooms, turnstiles, parking gates etc) that the subscriber desires to enter. The logical resource is typically a location on the network (computer workstations, folders, files, database records, software programs etc), that the subscriber desires to gain access to.

The authorization data component for both the physical and logical resource is populated with relevant subscriber access information. An example of this can be a simple Access Control List (ACL).

The physical and logical access controls are responsible for granting or denying access to a particular physical or logical resource respectively. The physical or logical access control interacts with the authorization data component to match the subscriber’s provided information to the information on record and either grant or deny access. The components typically interface with the card reader, the authorization data and optionally with the biometric reader, PIN Pad device and card/certificate status services to provide or deny physical or logical access.

4.3 Card Lifecycle Activities

The PIV card lifecycle primarily consists of seven activities:

- PIV card request: This activity deals with the initiation of a request for the issuance of a PIV card to an applicant by the PIV Requesting Official as well as the validation of this request by the PIV Authorizing Official.
- Identity proofing and registration: The goal of this activity is to prove that a claimed identity is truthful (i.e. authentic) and that he/she matches the entire set of identity source documents presented at the time of registration. On successful validation of these documents, the applicant is enrolled into the Agency's PIV Management System.
- PIV card issuance: This activity primarily deals with the personalization (physical and logical) of the card along with updating of the relevant registration databases.
- PKI credential issuance: This activity deals with generation of asymmetric key pairs and the issuance and loading of the necessary PKI certificates onto an applicant's PIV card.
- PIV card usage: The main purpose of issuing a PIV card is so that a cardholder can be authenticated or verified at a later point in time before providing physical or logical access. Access authorization decisions can then be made once the cardholder is successfully authenticated as part of this phase.
- PIV card maintenance: This activity deals with the maintenance or update of the physical card as well as the data such as various card applications, PIN, PKI credentials and biometrics stored on it.
- PIV card termination: The termination process is used to permanently destroy or invalidate the usage of the card including the data on it including the keys such that it cannot be used again.

The activities that take place at the time of fabrication and pre-personalization of the card at the manufacturers are not considered a part of this lifecycle model. The figure below presents these PIV phases and shows the PIV card request as the initial activity and PIV card termination as the end of life. Additional detail regarding system certification and accreditation and card revocation are provided in Section 9.

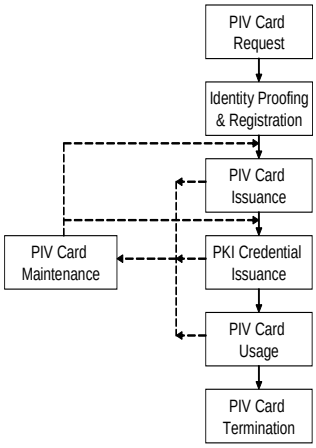


Figure 4-2: PIV Card Lifecycle Activities

5. PIV ISSUANCE

5.1 PIV Application and Approval for New Employees

An applicant shall apply for a PIV card as a part of the vetting process for Federal employment. A *PIV Requesting (Sponsor?) Official* shall submit the *PIV Request Form* for the Applicant. A *PIV Authorizing Official* shall approve the request and forward it to the *PIV Registration Authority*.

The PIV Request Form shall include:

- Name, organization and contact information of the PIV Requesting Official;
- Name, position including the position sensitivity level, and contact information of the Applicant including address of Applicant's parent organization;
- Name, organization and contact information of the PIV Authorizing Official,
- Name and contact information for the issuing organization,
- Signatures of the Requesting Official and the Authorizing Official.

Based on the required position sensitivity level, the Applicant shall complete the appropriate form listed Table 5-1.

Table 5-1: Forms Required from Applicant

Position Sensitivity Level	Form
1	Form I-9, OMB No. 1115-0136, Employment Eligibility Verification
2	Standard Form 85, OPM Questionnaire for Non-sensitive Positions
3	Standard Form 85 P, OPM Questionnaire for Public Trust Positions
4	Standard Form 85 P, OPM Questionnaire for Public Trust Positions

The Applicant shall provide the completed form to the Registration Authority. In addition, the Applicant shall appear in person and provide two forms of identity source documents from the list of acceptable documents included in the Form I-9 (reference) to the Registration Authority. At least one of the documents must be a valid State or Federal government-issued picture ID. The Registration Authority shall visually inspect the identification documents and authenticate them as being acceptable. In addition, the Registration Authority shall compare the picture on the source document to the applicant to ensure the applicant is the holder of the identity source document. At this time, the Registration Authority shall fingerprint the Applicant by collecting all of the Applicant's fingerprints. The Registration Authority shall conduct the appropriate background check as defined in Table 5-2 using the position sensitivity level from the PIV Request Form for the Applicant. Two of the Applicant's fingerprints shall be securely maintained for

personalization of the Applicant's PIV card. The Registration Authority shall also photograph the Applicant for personalization of the PIV card. After successful completion of the appropriate background check, the Registration Authority shall notify the Issuing Authority that a PIV card can be issued to the Applicant.

The Registration Authority shall be responsible to maintain:

- Completed and signed PIV Request Form,
- Copies of the identity source documents,
- Completed and signed background form received from the Applicant,
- Results of the required background check,
- Any other materials used to prove the identity of the Applicant.

Table 5-2: Background Checks By Position Sensitivity Level

Position Sensitivity Level	**Personal Identity Background Checks**
1 Low	Authentication of Applicant Identity Source Documents conducted by entity responsible for authorizing PIV card issuance (checking and verifying validity with each Document's Issuer). Law enforcement check (fingerprint).
2 Moderate	National Agency Check and Inquiries (NACI)[1]
3 High	NACI and Credit Check (NACIC)[2]
4 Critical (Vital National Asset-Critical Infrastructure)	Limited Background (LBI)[3] or Background Investigation (BI)[4]

[1] National Agency Check and Inquiries (NACI) – The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes:

- Employment 5 years
- Education 5 years and highest degree verified
- Residence 3 years
- References
- Law Enforcement 5 years
- NACs

The NAC is a part of every background investigation. Standard NACs are: Security/Suitability Investigations Index (SII), Defense Clearance Investigation Index (DCII), FBI Name Check, FBI National Criminal History Fingerprint check.

[2] NACI and Credit (NACIC) – This NACI includes the addition of a credit record search.

[3] Limited Background Investigation (LBI) – This investigation includes a NACIC, personal subject

5.2 PIV Application and Approval for Current Employees

A similar application and approval process shall be followed for current employees expect that background checks are not required if the results of the most recent previous check are on-file and can be referenced in the application and verified by the Registration Authority.

5.3 Card Issuance

The issuing organization shall confirm the validity of the request and compare the recipient's documents as well as the physical appearance of the recipient to the data submitted by the parent organization. If the documents are proved authentic to the applicable sensitivity level and the identity request is deemed valid, the office begins the process of issuance.

The issuing organization shall collect photographs and fingerprints of the recipient. The recipient may also be asked to provide a PIN and a cryptographic certificate.[5] The identity card is initialized for the recipient and issued. Actual issuance may occur during the initial visit to the issuer or may occur at a later date.

Simultaneously during the issuing stage, the recipient's name, the issuer identity, the card number, and possibly PKI certificate identification information are enrolled and registered with the backend database that supports the PIV system. Depending on the infrastructure design, this backend may be centralized or decentralized.

---

interview, and personal interviews by an investigator of subject's background during the most recent three years. Coverage includes:

- PRSI Personal Subject Interview
- Employment 3 years
- Education 3 years and highest degree verified
- Residence 1 year
- References 1 year
- Law Enforcement 5 years
- Court Records 3 years
- Credit 7 years
- NACs

[4] Background Investigation (BI) – This is a more in-depth version of the LBI since the personal investigation coverage is the most recent five to seven years. This investigation is required of those going into "high risk" public trust positions. Coverage includes:

- PRSI Personal Subject Interview
- Employment 5 years
- Education 5 years and highest degree verified
- Residence 3 years
- Law Enforcement 5 years
- Court Records 5 years
- Credit 7 years
- NACs

[5] Note that the issuing agency is responsible for the necessary PKI certificate management.

5.4 PIV Renewal

An applicant shall apply for a PIV card renewal when a PIV card expires or if the card is compromised or lost. The parent organization shall verify that the employee remains in good standing and personnel records are current prior to renewing the card.

6. CARD AND READER SPECIFICATIONS

6.1 Physical Characteristics (ISO/IEC 7810)

6.1.1 Standard Compliance

The PIV ICC shall comply with physical characteristics as delineated in ISO 7816, ISO 7810, ISO 10373-1 and ISO14443-1 (for cards with contactless interfaces). Any manufacturing process required to meet the requirements in this specification will meet the ISO standards and shall result in a flat card.

6.1.2. Printed Material

The printing shall not rub off during the life of the card nor deposit debris on the plastic card printer rollers during printing and laminating.

6.1.3 Physical Security Tamper Evidence

A tri-modal or bi-modal optical structure may be embedded in the PVC material on the front of the cardstock that is transparent when looking at it directly and changes colors as the viewing angle changes. Based on visual inspection, the optical structure shall be free of defects, such as fading, discoloration, or contamination.

Additional physical requirements include the following:

- Card material: Card body shall be polyvinyl chloride (PVC) in the laminate construction
- For cards without contactless interfaces, card body shall accept Dye Diffusion Thermal Transfer (D2T2) and resin thermal transfer imaging on front and back of card body. For cards with contactless interfaces, card body shall accept reverse transfer print imaging on front and back of card body
- The card shall be 27 to 33 mil card thickness (prior to lamination) in accordance with the ISO standard.
- In addition to the ISO 7810, cards shall be subjected ANSI INCITS 322, Card Durability Test Methods. While the INCITS 322 test methods do not currently specify compliance requirements, the tests shall be used to compare durability and performance of cards from different manufacturers. Examples of the INCITS 322 tests include card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, magnetic stripe abrasion, temperature and humidity induced dye migration, ultraviolet light exposure, and a laundry test.
- Resistance to Chemicals: The card shall be resistant to chemical effects arising from use in a flight line environment. The reagents called out in section 5.4.1.1 of ISO/IEC 10373-1 shall be modified to include gasoline (87 Octane), Jet A, Hydraulic fluid (MIL-H5606 or equivalent), and mineral spirits (ASTM D235 or equivalent). Immersion time shall be 1 minute.

- Cleaning: Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water. The reagents called out in section 5.4.1.1 of ISO/IEC 10373-1 shall be modified to include a 2% soap solution. A card shall be deemed acceptable if it meets these cleaning requirements.
- Ultraviolet light: The card shall be subjected to actual, concentrated or artificial sunlight to appropriately reflect 2000 hours of Southwestern United States sunlight exposure IAW ISO/IEC 10373-1, Section 5.12. Concentrated sunlight exposure will be performed IAW ASTM G90-98, and accelerated exposure IAW ASTM G155-00. Alternatively, the card may be subjected to the ANSI INCITS 322 tests for UV and daylight fading resistance. After exposure, the card shall be subjected to the ISO 10373-1 dynamic bending test and shall have no visible cracks or failures. The card shall not malfunction after the dynamic bending evaluation.
- Lamination: The cardstock shall withstand the effects of high temperatures required by the application of a 1 mil polyester laminate on one or both sides of the card by COTS equipment. The cardstock provided shall allow production of a flat card IAW ISO 7810 after lamination of one or both sides of the card.
- Peel Strength: Due to the tamper-resistant features of some embedded Optically Variable Devices (OVDs), the Government accepts that the minimum peel strength requirement in ISO 7810 may not be met for the OVD patch in the layer of the cardstock that contains it. The minimum peel strength requirement will be addressed on a case-by-case basis. However, the remainder of the cardstock layer with the OVD and the remainder of the card body shall meet all requirements of ISO 7810.

6.2 Reader Specifications

6.2.1 Contact Reader Specifications

Contact card readers shall conform to ISO 7816 Standards for the card-to-reader interface. These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface.

6.2.2 Contactless Reader Specifications

Contactless card readers shall conform to ISO Standard 14443 [ISO 14443] for the card-to-reader interface. In cases where these readers are connected to general purpose desktop computing systems, they shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface. In physical access control systems where the readers are not connected to general purpose desktop computing systems, the reader-to-host system interface is not specified in this Standard. This is necessary in order to allow retrofitting of PIV readers into existing physical access control systems that use a variety of nonstandard card reader communications interfaces.

6.3 Logical Credential

6.3.1 Logical Credential Data Model

In order to support multiple assurance levels, the PIV Logical Credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity via the authentication mechanisms specified at each assurance level. These data elements collectively comprise the data model for PIV Logical Credentials, and include the following:

- A Cardholder Unique Identification object (CHUID), mandatory
- A Global Personal Identification Number (PIN), mandatory
- Two biometric fingerprints, mandatory
- Biometric facial image, mandatory
- One (mandatory) or more (optional) asymmetric key pairs and associated certificates

PIV authentication objects fall into two categories: credential elements used to prove the identity of the cardholder to the card (CTC authentication), and credential elements used by the card to prove the identity of the cardholder to an external entity (CTE authentication) such as a host computer system. PINs fall into the first category, and the CHUID, biometric information, symmetric keys, and asymmetric keys fall into the second. Biometric information is not used in CTC authentication because the PIV architecture does not mandate on-card matching of biometric information.

The PIV data model may be extended to meet agency-specific requirements. A common extension may be support for one or more symmetric keys to be used locally for physical access control. Section 8.2.2 establishes algorithm and key size requirements for such keys. (Key management for such keys is not addressed in this standard, since interagency use is not envisioned.)

6.3.2 Data Formats

The PACS Implementation Guidance [PACS] defines a Cardholder Unique Identifier (CHUID). The PIV card shall include an elementary file container continuing the CHUID, as defined in [PACS], with two additions specific to this standard. In addition to the mandatory Federal Agency Smart Credential Number (FACS-N) that will uniquely identify a PIV card, the CHUID shall include an expiration date data element, that will specify in machine readable format when the card expires, to facilitate status checking, and the asymmetric signature field. The expiration date was not included in [PACS]; this specification uses a tag that was reserved for future use for this data (see Table 6.1) and encoding rules (see Table 6.2).

Table 6-1: CHUID Additional Expiration Date Data Element

(Cardholder Unique Identifier) CHUID File / Buffer EF 3000 Always Read			
Data Element	**Tag**	**Type**	**Max. Bytes**
Expiration Date	35	Fixed	8
RFU	36-3C		

Table 6-2: CHUID Additional Data Element Definitions.

Data Element	Length (bytes)	Description
Expiration Date	8	Mandatory LTV record. Expiration date in format: mmddyyyy

In addition, [PACS] does not specify a format for the asymmetric signature field. For PIV cards, the format of the asymmetric signature field is specified in Section 8.4 of this document.

Biometric information stored on the PIV card shall be encoded in the interchange format defined in [CBEFF]. Mechanism specific standards (i.e., for fingerprint images and facial images) are identified in Section 6.4. All biometrics stored on the PIV card shall be digitally signed. CBEFF defines a field for the signature but does not specify a format. For biometrics stored on PIV cards, the format of the asymmetric signature field is specified in Section 8.5 of this document.

The format of public key certificates shall be as defined in [RFC 3280]. Specific requirements by key type are described in *Annex B: Public Key Infrastructure for the PIV Card*.

The internal format of cryptographic keys stored on the card is not specified in this Standard.

6.3.3 File Structure

The PIV card architecture described in [SP800-xx] defines a Cryptographic Information Application (CIA) in Section 6 that contains information about cryptographic keys and other authentication objects that comprise the PIV cardholder's Logical Credentials. A host system can obtain all the information it needs to locate and retrieve biometric information from the card, or to select specific cryptographic keys stored on the card for subsequent cryptographic computations used in challenge-response operations. The host system can therefore dynamically discover the location and file identifiers associated with the Logical Credentials data elements, without the need for a priori knowledge of these. However, the CHUID and biometric information shall be stored as transparent files in the root file system of the Card Manager (the Master File) to facilitate rapid retrieval for physical access control applications.

It is important to note that the CIA may contain information about other authentication

objects associated with applications on the PIV card that are not specified in this Standard. This Standard only addresses authentication objects that are part of the PIV Logical Credentials.

6.4 Biometric Interfaces and Formats

Fingerprint is the only biometric information that will be used in both the processes. Face image will be used only for situations where fingerprints are difficult to acquire. The reason for limiting to these two types of biometric information is that the availability of large operational samples has enabled prediction of matching accuracy. No such large example exists for other types of biometric information like Iris Scan data. Also scanning systems for face and fingerprint images can operate with 0% FAR (Failure to Acquire Rates). This rate is unknown for Iris Scans. Further there are no open standards for Iris templates (the only one Iris template is proprietary) and the standard for exchange of image-based Iris scans information is still not mature.

The format for the storage and exchange of the biometric information captured and used in PIV system must conform to established standards in order to improve our confidence in the fingerprint matching (recognition) system as well as the usability of exchanged information. In the PIV system, fingerprint matching is done in the following stages.

- PIV Card Approval: As part of the PIV card application process, fingerprint information is collected from the PIV card applicant. Then the identity proofing process begins. The tasks involved in identity-proofing are incremental with each level of the registration assurance which in turn depends upon the position sensitivity-level of the Federal employee or contractor. Verification of I-9 source documents and use of fingerprint for law enforcement check are the common tasks in all registration assurance levels. The law enforcement check is performed by comparing the fingerprint information collected from the PIV card applicant with those in the government archival databases (e.g., STATE INDEX – 6M images, IAFIS – 1.2M images). This One-to-Many matching is called “IDENTIFICATION” in the biometric parlance. In this document, we will use the term “Biometric Identification” in order to differentiate it from the term “identification” that is widely used in other parts of this document.
- PIV Card Authentication: The fingerprint information stored in the PIV card is extracted by the PIV card authentication system. The fingerprint information from the PIV cardholder is obtained through a live scan. The One-to-One matching of these two fingerprint information establishes the fact that the card user is the legitimate cardholder. This One-to-One matching is called “VERIFICATION” in biometric parlance. In this document, we will use the term “Biometric Verification” in order to differentiate it from the generic term “verification”. The One-to-One matching establishes the binding between an identity marker (fingerprint biometric information) and the individual and thus authenticates the cardholder to the card. PIV Card authentication may be augmented by verifying the digital signature on the biometric (see Sections 6.4.2 and 8.5). The digital signature is computed over the biometric data and the FASC-N that uniquely

identifies the PIV card. By verifying the signature, the PIV card authentication system can verify that the biometric data was recorded by a PIV registration system during card issuance and stored on the presented PIV card

6.4.1 Fingerprint Information Category Selection

Biometric Identification and Biometric Verification using fingerprints can involve information in one of the following categories:

- Raw or Processed Image
- Minutiae
- Patterns

Raw fingerprint images are the ones obtained by scanning and contain detailed pixel information. They form the first point of capture of any fingerprint information. Processed fingerprint images contain fewer pixels and fewer grayscale levels. This type of information is used to reduce the storage requirements. Minutiae and Patterns are nothing but different fingerprint characteristics. They require the use of a high quality fingerprint image for their generation. Characteristic-based (minutiae or patterns) fingerprint information requires even less storage space than image-based (raw or processed) fingerprint information. Fingerprint information based on either minutiae or patterns formats cannot be used by matching algorithms designed to use the other format. Even within the same characteristic (say minutiae), there is interoperability problem when information is exchanged between two systems. For example, in order to use minutiae data as the interchange medium for fingerprint information between different fingerprint matching systems, the minutiae information (a form of template) must be extracted (features defined and located) from a fingerprint image and then encoded (formatting and representation) and sent to the matching system. The matching system compares the received template (called probe template) with the database of templates (called gallery templates) using a matching algorithm. There are now many proprietary approaches with respect to extractors, encoding schemes and matching algorithms. Hence there is no confidence in the reliability of the match produced using the data interchanged between dissimilar minutiae matching systems. NIST is now in the process of gathering data and equipment to perform the Minutiae Interoperability Exchange Test [MINEX04]. The purpose of the test is to determine the various combinations of template schemes, probe templates, gallery templates and fingerprint minutiae matchers that will produce successful matches. Pending this test, as of now, it is an established fact that the interchange of fingerprint image data provides the greatest interoperability between dissimilar fingerprint recognition systems. It provides implementers of these systems the flexibility to accommodate images captured from dissimilar devices, varying image sizes, resolutions and different grayscale depths. It also provides freedom in the choice of the matching algorithms (can be image-based, minutiae or patterns-based).

6.4.2 Fingerprint Data Requirements for PIV Card Approval

This standard requires capture of images from ten fingers for the purpose of PIV card

approval. NIST studies using IDENT (the fingerprint matcher from US-VISIT) [NISTIR 7110] have shown that images containing index finger pairs can provide 96% TAR (Total Accuracy Rate - the matching accuracy measure) with 0.09% FAR (Failure Acquisition Rate) on a database with up to 6 million images for the purpose of biometric identification (one-to-many matching for law enforcement check). However the TAR drops to 53.6% for low quality images. Since image quality of most archival law enforcement databases is lower than the image quality in US-VISIT data, the strategy for improving matching accuracy is to increase the number of fingers used. Since another NIST study [NISTIR 7116] has shown that a typical 10-finger fingerprints (using accurate COTS system) yields a TAR of 99.95% at a FAR of 0.01%, the use of slap(flat) images from all 10 fingers is prescribed for PIV card approval.

The overall format for recording, storing and transmitting the information together with content and units of measurement shall be as specified in the ANSI INCITS 381-2004 standard. The captured images shall be a plain impression image (also called slap or flat) - obtained from fingers placed on a platen without any rolling movement.

- The fingerprint information for all 10 fingers shall be captured through three multi-finger images. The three multi-finger images are: (a) combined impression of the four fingers of the right hand (except the thumb) (b) combined impression of the four fingers of the left hand (except the thumb) and (c) combined impression of the left and right thumbs. The location of the fingers within the overall fingerprint image in a multi-finger image shall be as specified in Section 6.7 of ANSI/INCITS 381-2004. The maximum size for each of these three types of recorded images shall be as defined in Table 6 and Table 19 of ANSI/NIST-ITL 1-2000 standard and referenced through codes 13, 14 and 15 respectively in Table 5 of ANSI/INCITS 381-2004.
- The scanning resolution used for image capture should be such that the output (delivered) image from the scanning system has a resolution of 500 pixels per inch (ppi), plus or minus 5 pixels per inch, with each pixel represented by 8 bits (256 grayscale levels). These requirements are met by “Acquisition Setting Levels” 30,31, 40 & 41 of INCITS 381-2004. Systems using levels 30 & 31 are the ones widely deployed in law enforcement applications and out of which Level 31 is recommended in this standard since it requires certification contained in Appendix F of the FBI’s Electronic Fingerprint Transmission Specification (EFTS/F). A certified version of Wavelet Scalar Quantization (WSQ) method for 8-bit 500 ppi grayscale image is the recommended compression algorithm.
- The image quality for flat fingerprint images submitted to FBI for law enforcement check should be specified using the NIST NFIQ scale [NISTIR 7151]. The NIST Image Quality Level must be supplied through a Finger Image Quality field in the Finger Image Header record. This is a mandatory requirement for all slap (flat) fingerprint submissions to the FBI database from March 2005.

ANSI-INCITS 381-2004 not only specifies the format and content for an individual finger record but also stipulates that the record be embedded within a Common Biometric Exchange File Format (CBEFF) [NISTIR 6529-2001]. The three fingerprint records

(corresponding to each of the three fingerprint images) will be embedded in a CBEFF-compliant data structure for transmitting to the FBI database for law enforcement check. The identification that the finger records conform to ANSI INCITS 381-2004 format should be provided in the CBEFF embedding record (the wrapper) through the Format Owner and Format Type Code fields with values 0x001B (decimal 27 – INCITS M1 committee) and 0x0401 (decimal 1025 – fingerprint image) respectively.

Table 6-3: Biometric Information Requirements for PIV Card Approval

Biometric Information Property	Property Metric
Representation Type	Compressed Image
Compression Algorithm	WSQ
Resolution	500 ppi or higher
Grayscale Value	8 bits Minimum
Number of fingers	All 10 fingers
Impression Type	Live-scan plain (or) Nonlive-scan plain[6]

6.4.3 Fingerprint Data Requirements for PIV Card Authentication

This standard requires capture of images from two index fingers (one from each hand) for the purpose of PIV card authentication. NIST studies from INS data [NISTIR 7123] has shown that one index fingerprint can provide 90% TAR (Total Accuracy Rate - the matching accuracy measure) with 0.1% FAR (Failure Acquisition Rate) and 1% probability of false acceptance using current commercial technology for the purpose of biometric verification (one-to-one matching for PIV card authentication). The matching accuracy improves to 99.6% TAR for the same FAR and false acceptance parameters when the two index fingers are used [NISTIR 7110] (using the US-VISIT two fingerprint matching system).

As in the case of fingerprints acquired for card approval, the overall format for recording, storing and transmitting the information together with content and units of measurement shall be as specified in the ANSI INCITS 381-2004 standard. The captured image again shall be a plain (flat) impression image. The compression algorithm, image resolution and pixel depth (number of bits used for gray levels) shall be the same as those used for fingerprints acquired for PIV card approval process. They are reproduced in a Table 6-4 for completeness.

[6] Small agencies or field offices may not have fingerprint scanners to produce fingerprint to the specs specified in FIPS 201. These agencies may gather fingerprints through ink on card. For submission to law enforcement check however electronic fingerprints are required.

Table 6-4: Biometric Information Requirements for PIV Card Authentication

Biometric Information Property	Property Metric
Representation Type	Compressed Image
Compression Algorithm	WSQ
Resolution	500 ppi or higher
Grayscale Value	8 bits Minimum
Number of fingers	Two Index Fingers
Impression Type	Live-scan plain

6.4.4 Face Image as the Alternate Biometric Information

This standard allows the use of face image as the biometric information for PIV identity-proofing and PIV card authentication as an alternative measure. The alternative is to be used in the case of subjects who cannot be fingerprinted. It has been found in a study that about 2% of the population has damaged fingerprints. Also people may have missing fingers.

As in the case of fingerprints, only image-based data will be used since there are no accepted templates for face – minutiae or patterns. The illumination under which the face image is captured determines its quality. Yet another determinant of face image quality is the pose – the angle between the camera and the face. Face image captured under outdoor illumination is of poor quality while that captured using controlled illumination is of a high quality if other factors such as the sophistication of image capture device are the same.

The record format together with contents and units of measurement for face images used for PIV card approval and authentication should conform those specified in ANSI INCITS 385-2004. The minimal resolution should be 600 ppi and JPEG is the recommended compression algorithm.

- Face Image for PIV Card Approval: NIST studies have shown [NIST 7110] that for biometric identification (one-to-many matching used for law enforcement check (in our case for PIV card approval)) using face images, the matching accuracy decreases with database size (also called gallery size) even for high quality facial images. These results should be borne in mind when using face images as a law enforcement checks. One of the archival databases used for biometric identification is the STATE database with 6.3M images.
- Face Image for PIV Card Authentication: NIST report [NISTIR 7110] has shown that for biometric verification (one-to-one matching for PIV card authentication), there is a significant drop in matching accuracy (to around 50%) when the face images are captured using outdoor or uncontrolled illumination as opposed to those captured using controlled illumination. Specifically the outcomes showed that for the best 2002 face recognition system TAR at 1% FAR was 90% using controlled illumination [NIST 7110] while the best TAR dropped to 54% at 1% FAR when outdoor illumination was used [NISTIR 6965]. Also it has been found

that the TAR for the most accurate commercial face recognition systems is far less than those of the most accurate commercial fingerprint recognition systems [NISTIR 7110]. In view of this, the facial image will only be used for human verification (manual authentication in our PIV system).

6.5 Topography

Section 6.1 provides a description of the physical characteristics of the PIV Card, and the applicable standards. This section discusses the visual content and layout of the PIV Card.

The issuer provided information in a PIV card shall be in both visual and electronic form. No information on the PIV card will be embossed. This section does not cover information stored in ROM and accessible only through ICC. The side of the card that contains the contacts (in the case of 7816 cards) is referred to as the front of the card and the other side is referred to as the back of the card. The mandatory information together with the associated layout and identity verification functions are stated under the Mandatory Topography section (section 6.5.1 below). The combination of mandatory and optional information and the resulting layout are described in section 6.5.2 (Enhanced Topography).

6.5.1 Mandatory Topography

6.5.1.1 Front of the Card:

The pictorial representation of the mandatory and optional visual information on the front of the card is given below. The description of each mandatory information item follows.

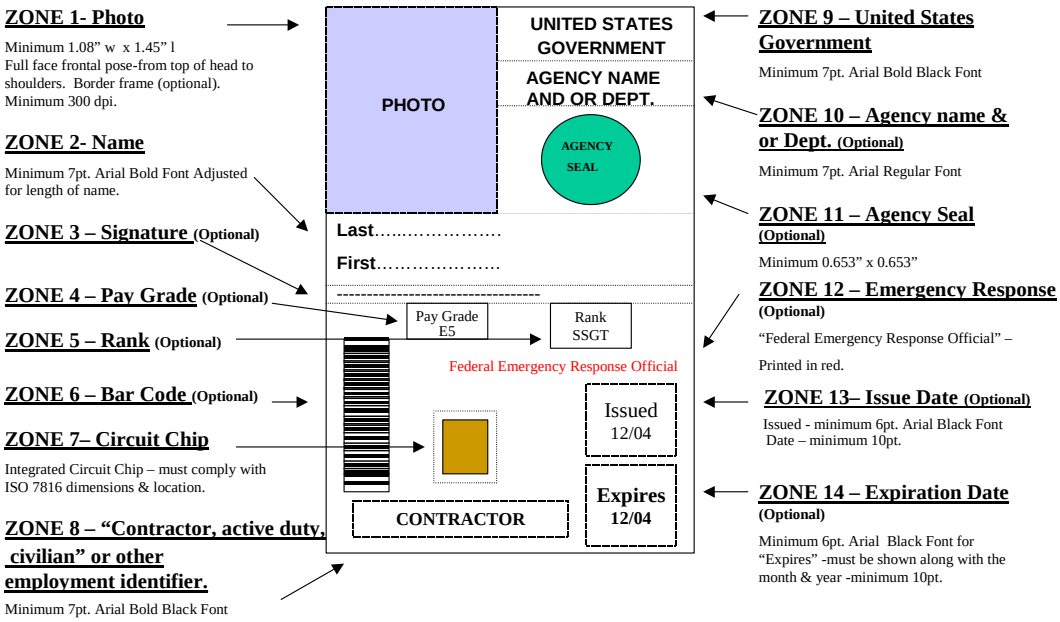


Figure 6-1: Front of the PIV Card

Photograph (Mandatory) — The photograph shall be placed in the upper left corner on the front of the card. Alternatively, the photograph shall be placed in the center (in a way not interfering with the contact chip location) on the front of the card. The photograph shall be a full frontal pose from top of the head to shoulder and shall be, at a minimum, 1.08 inch wide and 1.45 inch in length (the larger the photograph, the more useful it will be for visual verification). A minimum of 300 dpi resolution is required. Border frame is optional.

Name (Mandatory) — The names shall be printed under the photograph in all capital letters. The font shall be Arial Bold of minimum 7pt size.

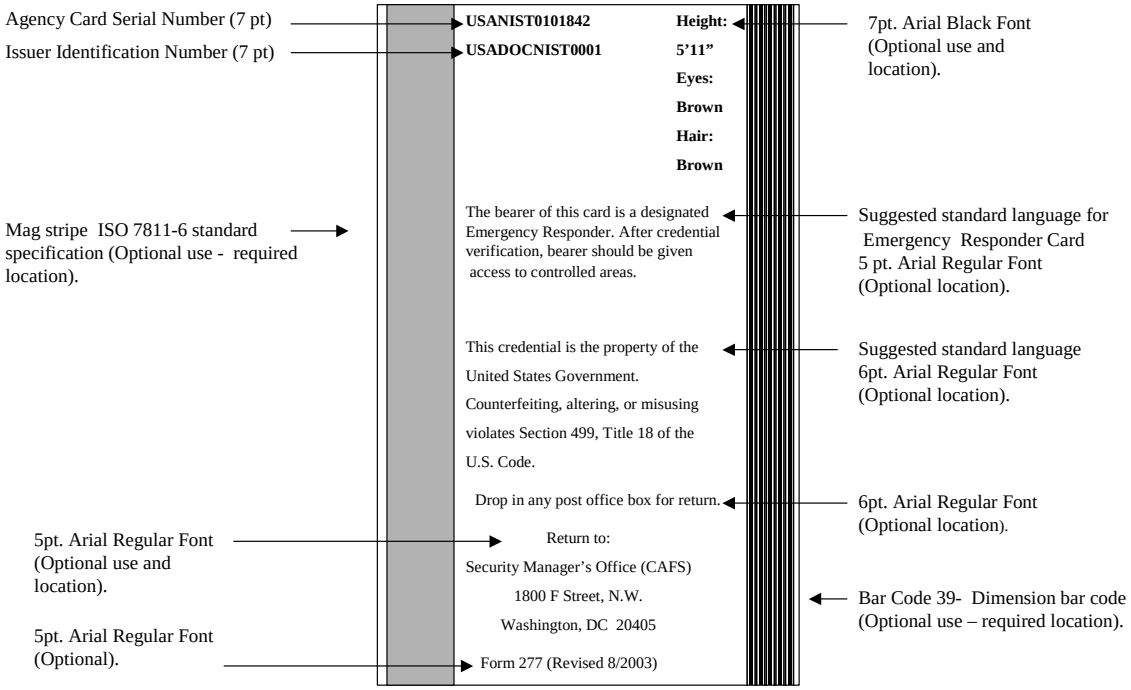
Contractor or Other Employment Identifier (Mandatory) — The bottom front part of the card shall print the letters "CONTRACTOR," "ACTIVE DUTY", "CIVILIAN" or an Agency-specific employee identifier". The font shall be Arial Bold Black of minimum 7 pt size.

United States Government (Mandatory) — The "UNITED STATES GOVERNMENT" text shall be printed on the top front portion of the card. The font shall be Arial Bold Black of minimum 7 pt size.

6.5.1.2 Back of the Card:

The pictorial representation of the mandatory visual information on the back of the card is provided in Figure 6-2. The card issued to the military follows the Geneva convention format rather than the standard PIV format as depicted in Figure 6-3. The description of all visual information items follows.

Figure 6-2: Back of the PIV Card



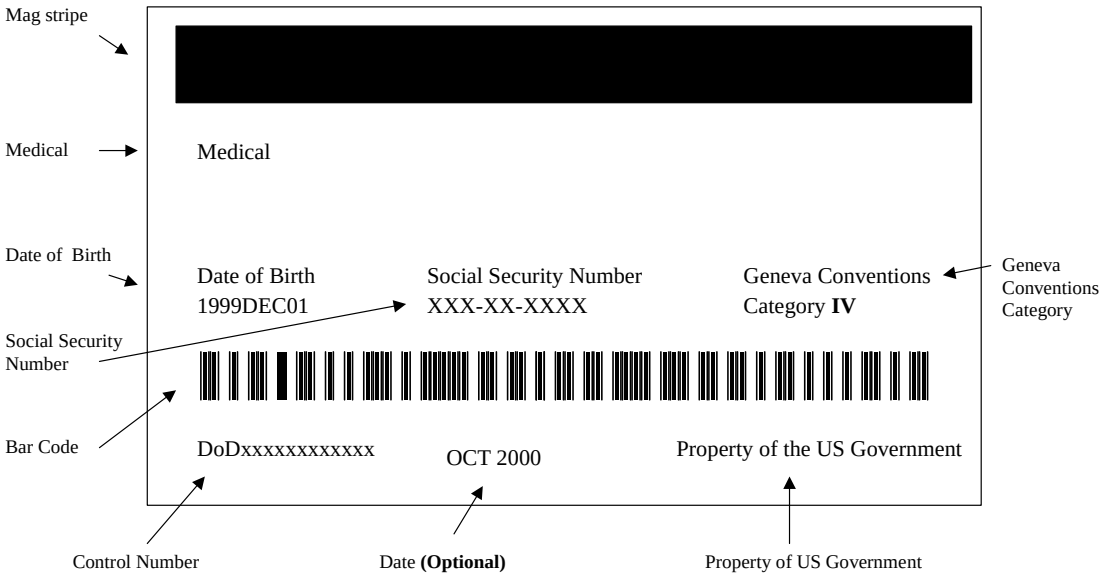


Figure 6-3: Back of the Military PIV Card

Agency Card Serial Number — The first line on the back of the card shall print the card's unique serial number in the context of the issuing Agency. The format for this serial number will be left to the discretion of the issuing Agency.

Issuer Identification — The second line on the back of the card shall print the issuer identifier, which comprises of six characters of Department code and four characters of Agency code, followed by a five digit number that uniquely identifies the issuing facility within the Agency.

6.5.2 Optional Topography

A PIV token with enhanced topography consists of both mandatory and optional information. The description of optional information on the front surface of the card (as shown in Figure 6-1) follows.

6.5.2.1 Front of the Card:

The pictorial representation of a PIV Card with enhanced topography (consisting of both mandatory and optional information) is depicted in Figure 6-1. The description of optional information follows:

Signature — The agency may print the cardholder signature below the photograph and cardholder name. The space for the signature should not interfere with the chip location.

Pay Grade — The pay grade for the cardholder may be printed here in a format determined by the issuing Agency.

Rank — The rank the cardholder may be printed here in a format determined by the issuing Agency.

Bar Code — A bar code may be inserted in the left side of the card surface if applicable to the issuing Agency.

Agency Name & or Dept. — The name of the Agency and the cardholder's department may be printed here. The font shall be Arial Black of minimum 7pt size.

Agency Seal — The seal for the issuing Agency may be printed on the upper right side of the card. The font shall be Arial Black of minimum 7pt size.

Emergency Response Official Identification — The agency may print "Federal Emergency Response Official" above the chip in red color.

Expiration Date — The date of card expiry may be printed in the lower right hand corner of the card in the month/two digit year format. The font for the text "Expires" shall be Arial Black of minimum 6 pt size. The font for date shall be Arial Black of minimum 10pt size.

Issue Date — The date of card issuance may be printed above the expiration date in the month/two digit year format. The font for the text "Issued" shall be Arial Black of minimum 6 pt size. The font for date shall be Arial Black of minimum 10pt size.

6.5.2.2 Back of the Card:

The description of optional information on the back surface of the card (as shown in Figure 6-2) follows.

Holder's Physical Characteristics — The cardholder's physical characteristics such as height, eye color, and hair color may be printed on the back of the card in Arial Black font of minimum 7 pt size. Moreover, these physical characteristics may be digitally stored on the storage medium.

Standard Language for Emergency Responder — The standard language for emergency responder may be printed on the back of the card in Arial Regular font of minimum 5 pt size. The printed statement should read "The bearer of this card is a designated Emergency Responder. After credential verification, bearer should be given access to controlled areas."

Standard Section 499, Title 18 Language — The standard Section 499, Title 18 language warning against counterfeiting, altering, or misusing the card shall be printed below the issuer identification in Arial Regular font of minimum 6 pt size.

Instructions for Return of Lost Token — The card shall print the return address and instructions in case the card is lost. The bottom back of the card is designated for these purposes. The font used for instruction information shall be Arial Regular front of minimum 6pt size. The front used for return address information shall be Arial Regular of minimum 5 pt size.

Form Number — The bottom back of the card may print form number in one line using Arial Regular front of minimum 5 pt size.

Magnetic Stripe — The card may optionally have a magnetic stripe. The magnetic stripe should be placed on the card in accordance with ISO 7811.

Bar Code 39 Dimension Bar Code — The left corner (from top to bottom) on the back of the card may be used to print bar code. The data encoding should be done using Bar Code 39 scheme. However, the data stored will not be standardized by FIPS 201.

6.6 Cryptographic Security Functions

At a minimum, the PIV card must store one asymmetric private key, a corresponding public key certificate, and perform cryptographic operations using the asymmetric private key. Cryptographic operations with this key are only performed through the contact interface, as specified in Section 8.2.1.

Asymmetric private keys shall be 1024 or 2048 bit RSA keys, or elliptic curve keys of corresponding strength. The only cryptographic operation that is required is the RSA

decrypt function or the elliptic curve sign function.

Optional functions supporting this key are:

- RSA key pair generation; and
- Trust anchor certificate storage.

The PIV token may include additional asymmetric keys and PKI certificates. This specification defines requirements for digital signature and key management keys. Where digital signature keys are supported, the PIV card is not required to implement a secure hash algorithm (e.g., SHA-1). Message hashing may be performed off card. As above, useful optional functions include key pair generation and trust anchor storage.

No cryptographic operations are mandated for the contactless interface, but the CHUID contains data signed by the PIV Card Management system. Agencies may choose to supplement the basic functionality with storage for a local authentication key (see 8.2.2) and support for a corresponding set of cryptographic operations. That is, if an agency wishes to utilize an AES-based challenge response for physical access, the PIV card must contain storage for the AES key and support AES operations through the contactless interface. If the contactless interface utilizes asymmetric cryptography (e.g., elliptic curve cryptography), the PIV card may also require storage for a corresponding public key certificate.

Requirements for the storage and protection of private keys on the PIV card are detailed in Section 8.

7. PIV VERIFICATION INFRASTRUCTURE

The PIV infrastructure is intended to provide PIV card and key status information across agencies and organizations, to support high assurance interagency PIV card interoperation, while minimizing the needed infrastructure and concentrating the responsibility for implementing operating the service in the shared service provider CAs. Agencies will be responsible for issuing PIV Cards and the associated processing, for implementing the physical and logical access control systems that use the PIV cards, and notifying CAs when cards or certificates are revoked, unless they operate their own CAs. A small number of shared service provider CAs, and legacy Agency CAs will issue all Federal authentication certificates and maintain the status servers and responders needed for PIV card and certificate status checking.

PIV smartcards shall contain an authentication public key certificate and its associated private key, as well as a Cardholder Unique Identifier (CHUID), defined in [PACS]. The public key certificate shall be accessed via the ISO/IEC 7816 contact interface, while the private key may be invoked for signing operations via the contact interface, after the card has first been activated by entering a PIN. The CHUID is normally accessed through the ISO/IEC 14443 contactless interface, without explicit user activation of the card.

Authentication certificates, as specified in Annex B, contain the cardholder's agency, name and other distinguishers as required in the subjectName field of the card, and also include the a field extracted from the CHUID, the Federal Agency Smart Card Number (FASC-N) in a subject alternate name extension. The FASC-N is the card number and includes an agency code. The expiration date of the authentication certificate shall not be after the expiration date of the PIV card. If the card is revoked, the authentication certificate shall be revoked. However an authentication certificate (and it's associated key pair) may be revoked without revoking the PIV card, and may then be replaced. A current, unexpired PIV authentication certificate on a card is proof that the card was issued and is not revoked, and a successful cryptographic proof of possession (POP) test of the associated private key proves that the card is valid, without revealing the key to the card validator.

The authentication certificate and private key may be used in the usual fashion for logical authentication to local or remote information systems, with authentication protocols such as client-authenticated TLS, that are implemented in virtually every browser. This standard doe not specify a specific public key authentication protocol. The authentication certificate and private key may also be used to validate cards for access to facilities. In these scenarios, the user inserts his card in an access control reader, and enters his PIN, which activates the card. The access control system reads the certificate from the card, and requests the card to sign a challenge with it's private key. If the signed reply is valid, then the card is validated, and the PIN confirms is that the person with the card is the actual user named on the access certificate. The normal PKI certificate status mechanisms, described below, can then be used to confirm that the certificate (and therefore the card) is current and has not been revoked. Note that this can be done at the

entry control access point to a building, or in advance remotely, when a prospective visitor is registering his visit with the agency to be visited.

Since the lifetime of authentication certificates is long, typically several years, a certificate revocation mechanism is necessary. Two are conventional: the Certificate Revocation List and the On-line Certificate Status Protocol (OCSP). CAs that issue PIV authentication certificates shall maintain a Lightweight Directory Access Protocol (LDAP) directory server that holds the CRLs (See Appendix E) for the certificates it issues, as well as any CA certificates needed to build a path to the Federal Bridge CA. Certificates shall contain the crlDistributionPoint or authorityInformationAccessPoint extensions needed to locate CRLS and the authoritative OCSP responder. Since the cardholder's certificate is always available on the PIV card, there is no need for the LDAP server to provide user certificates. In addition every CA that issues PIV authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues. Access control points may use either the CRLs or the OCSP responder to check certificate status, as best meets their needs.

In addition to the authentication certificate, all PIV cards shall support the PACS CHUID defined for the Medium Assurance Profile, with one extension defined below, a card expiration date. The three PACS assurance profiles can be summarized as:

- Low Assurance: Supplies the CHUID as an unsigned string
- Medium Assurance: The CHUID is signed
- High Assurance: In addition to acting as a storage card for the CHUID, the card holds several symmetric keys and uses them to generate authentication replies to challenges.

PIV cards shall support the PACS CHUID Medium Assurance Profile extended to contain a card expiration date, via the ISO/IEC 14443 contactless interface. Since the Low Assurance Profile is a subset of the Medium Assurance profile it is also realized if access control points choose to not verify signatures. Because PACS does not yet specify how to access this feature through he the ISO/IEC 14443 contactless interface, and because the secure management of symmetric keys is difficult, support for the high assurance profile is optional, and agencies may choose to implement it in their cards, provided that a FIPS approved block cipher is used in a FIPS validated cryptographic module. Therefore agencies should not expect to use the PACS High Assurance Profile to authenticate visitors from other agencies, however they may choose to implement the High Assurance Profile for their own employees and contractors.

The PACS Low and Medium Assurance Profiles require only storage cards, while the High Assurance Profile requires a cryptographic processor as well. Since only storage capability is required for the low and medium levels, agencies may choose to provide the CHUID on other storage media such as magnetic or optical stripes, as well as through the ISO/IED 14443 contactless chip interface. However, agencies should not assume that visitors from other agencies will have any CHUID interface except ISO/IEC 14443.

The CHUID/FACS-N mechanism assumes that access control points will be pre-provisioned with an access control list (ACL) of permitted FASC-Ns. Anyone with a card with that FASC-N is permitted to pass (subject, according to local policy, to automatic biometric checks or human card photos). At the Medium Assurance Profile the CHUID is signed, so the access point knows that the card was issued and is not a complete fabrication, while the expiration date allows confirmation that the card has not expired. Status checking, if done, must take place in the creation and maintenance of the ACL. Since the authentication certificate also includes the FASC-N, status checking can be done through the certificate status mechanisms at a visitor's entry point, or remotely in advance, if the prospective visitor registers at a visitor registration website with his or her PIV card. The provisioning and management of physical access ACLs is outside the scope of this FIPS. .

8. CRYPTOGRAPHY REQUIREMENTS

8.1 PIN

To unlock the contact interface of the PIV Card, the cardholder shall supply a numeric PIN. The PIV card shall include mechanisms to limit the number of guesses an adversary can attempt if a card is lost or stolen. The minimum PIN length shall be sufficient, to ensure that the maximum probability that an attacker no *a priori* knowledge of the password will succeed in an in-band password guessing attack is 2^{-14} (1 in 16,384).[7] For additional information, regarding this calculation, please refer to Appendix A in NIST SP 800-63, *Electronic Authentication Guideline*.

8.2 PIV cryptographic keys

The PIV card has single mandatory key and three optional keys:

1. The *PIV authentication* key is an asymmetric private key supporting logical and physical access and is mandatory for each PIV card;
2. The *Local authentication* key may be either a symmetric (secret) key or an asymmetric private key for physical access and is optional;
3. The *digital signature key* is an asymmetric private key supporting document signing and is optional; and
4. The *key management key* is an asymmetric private key supporting document signing and is optional.

All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above. All PIV cryptographic keys shall be stored within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV card shall provide Level 3 physical security to protect the PIV private keys in storage.

The PIV card performs all cryptographic operations using the PIV keys on card. The PIV card need not implement any additional cryptographic functionality. When used to protect access to sensitive data and systems, this functionality may be augmented (e.g., with hash algorithms and signature verification) by a validated software cryptographic module.

Algorithms and key sizes for each PIV key type are specified in the following table.

[7] This is consistent with a Level 2 password mechanism in NIST SP 800-63 and implies a minimum of a 6-digit PIN.

Table 8-1: PIV Key Type

PIV Key Type	Time Period	Algorithms & Key Sizes
PIV authentication key	Through 12/31/2010	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Local authentication key	Through 12/31/2010	Two Key Triple-DES (TDEA2) Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256 RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256 RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Digital signature key	Through 12/31/2007	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2007	RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Key management key	Through 12/31/2007	RSA/D-H 1024 bits or higher; ECDH 160 bits or higher
	After 12/31/2007	RSA/D-H 2048 bits or higher; ECDH 224 bits or higher

Requirements specific to each storage and access of each class of keys are detailed below. Where applicable, key management requirements are also specified.

8.2.1 The PIV Authentication Key

The PIV card shall not permit exportation of *PIV authentication* key. The PIV authentication key must be available only through the contact interface of the PIV card. Private key operations may be performed using an activated PIV card without explicit user action (i.e., the PIN need not be supplied for each operation.)

The PIV card shall store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate shall include the FASC-N in the subject alternative name extension to support physical access procedures. The expiration date of the certificate must be no later than the expiration date of the PIV card.. *Annex B: Public Key Infrastructure for the PIV Card* specifies the certificate format and the key management infrastructure for PIV authentication keys.

8.2.2 The Local Authentication Key

The PIV card shall not permit exportation of *local authentication* key. The local authentication key is used solely for physical access (e.g., to support PACS High

assurance authentication) and must only be available using the contactless interface of the PIV card. Private/Secret key operations may be performed using this key without explicit user action (i.e., the PIN need not be supplied.)

Cross-agency interoperability is not a goal for the local authentication key. Consequently, this document does not specify key management protocols or infrastructure requirements.

8.2.3 The Digital Signature Key

The PIV card shall not permit exportation of the digital signature key. If present, the digital signature key must only be accessible using the contact interface of the PIV card. Private key operations may be performed using an activated PIV card with explicit user action (i.e., the PIN must be supplied for each private key operation.)

The PIV card shall store a corresponding X.509 certificate to support validation of the *digital signature* key. *Annex B: Public Key Infrastructure for the PIV Card* specifies the certificate format and the key management infrastructure for PIV digital signature keys.

8.2.4 The Key Management Key

The PIV card shall not permit exportation of the key management key in plaintext. If present, the key management key must only be accessible using the contact interface of the PIV card. Private key operations may be performed using an activated PIV card without explicit user action (i.e., the PIN need not be supplied for each operation.)

The PIV card shall store a corresponding X.509 certificate to support validation of the *key management* key. *Annex B: Public Key Infrastructure for the PIV Card* specifies the certificate format and the key management infrastructure for PIV key management keys.

8.3 PIV Cryptographic Operations

The PIV card performs all cryptographic operations using the PIV keys on card. The PIV card need not implement any additional cryptographic functionality. When used to protect access to sensitive data and systems, this functionality may be augmented (e.g., with hash algorithms and signature verification) by a validated software cryptographic module.

8.4 Asymmetric Signature Field in CHUID

This specification requires inclusion of the Asymmetric Signature field in the CHUID container. The Asymmetric Signature data element of the PACS CHUID shall be formatted as a detached PKCS#7 digital signature. The digital signature shall be computed over the entire contents of the CHUID, excluding the Asymmetric Signature field itself.

The CMS external digital signature must contain the following elements:

- Content shall be SignedData;
- Certificates and CRLs shall not be included in the message;
- The Signed Attributes field shall be present and shall include a single attribute. The attribute shall be a serialNumber and the value shall be the FASC-N.
- SignerInfos shall be present and include only a single SignerInfo;
- The SignerInfo shall:
  - Use the issuerAndSerialNumber choice for SignerIdentifier
  - Specify the Digest Algorithm;
  - The authenticated attributes shall be present and include
    - The cardholder's name;
    - The DN for the cardholder's PKI certificates; and
    - The CHUID for the physical card that the biometric was stored on
- Include the digital signature.

Digital signatures in public key certificates and CRLs shall be formatted as described in [RFC 3279]. Digital signatures in OCSP responses shall be formatted as described in [RFC 2560].

The following algorithm and key size requirements apply to the digital signature in the Asymmetric Signature field:

Table 8-2: Algorithm and Key Size Requirements

Card Expiration	Public Key Algorithms & Key Sizes	Hash Algorithms
Through 12/31/2007	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher	SHA-1 hash algorithm
Through 12/31/2010	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher	SHA-1, SHA-224 or SHA-256 hash algorithm
After 12/31/2010	RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher	SHA-224 or SHA-256 hash algorithm

The public key required to verify the digital signature shall be available as an X.509 certificate. The certificate shall be a digital signature certificate issued under the Common Policy, and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Annex B: Public Key Infrastructure for the PIV Card.

8.5 Protection of Biometrics

The mechanisms provided by the PIV card must protect biometric data in storage. Biometric data shall only be accessible using the contact interface of the PIV card. The

PIV card must be activated by the user before biometric data can be provided to the reader. Additional explicit user action is not required (i.e., the PIN need not be supplied twice) to permit access to the biometric data.

Signatures on biometrics stored on the PIV card shall be formatted as a CMS external signature, as defined in [RFC 3852]. The digital signature shall be computed over concatenation of the following CBEFF elements:

- CBEFF Header Version (If Present);
- Patron Header Version;
- Biometric Type (If Present);
- Record Data Type (If Present);
- Record Purpose (If Present);
- Record Data Quality (If Present);
- Creation Date (If Present);
- Creator (If Present);
- Biometric Specific Memory Block (BSMB) Format Owner;
- BSMB Format Type; and
- BSMB.

The CMS external digital signature must contain the following elements:

- Content shall be SignedData;
- Certificates and CRLs shall not be included in the message;
- The Signed Attributes field shall be present and shall include a single attribute. The attribute shall be a serialNumber and the value shall be the FASC-N.
- SignerInfos shall be present and include only a single SignerInfo
- The SignerInfo shall:
  - Use the issuerAndSerialNumber choice for SignerIdentifier
  - Digest Algorithm shall be
  - The authenticated attributes shall be present and include
    - The cardholder's name;
    - The DN for the cardholder's PKI certificates; and
    - The CHUID for the physical card that the biometric was stored on
  - Include the digital signature.

9. LIFE CYCLE MANAGEMENT

The preceding sections of this document establish a robust baseline for personal identity verification. However, while deployment of PIV cards and a supporting infrastructure that meets the technical specifications is the necessary first step, it is not sufficient. To ensure that the desired level of assurance for identity verification is achieved, appropriate policies must be established and performed by trustworthy and well-trained personnel.

Policies for card issuance were established earlier in this document. However, cards may not remain valid through their expiration date. The cardholder may retire, change jobs, or be fired, invalidating a previously accurate card. The PIV card system must ensure this information is distributed efficiently, both within the PIV management infrastructure and to parties authenticating a cardholder. Section 9.1, below, establishes policy requirements for PIV card revocation.

The policies for card issuance and revocation must be enforced throughout the PIV system to ensure the desired level of assurance is achieved. Before commencing operation, each PIV card issuer must undergo an accreditation process to ensure correct implementation of these policies. A systematic process with internal auditing and periodic re-accreditation is required to maintain this level of operation. Section 9.2, below, specifies requirements for certification and accreditation for the PIV card issuer. Section 9.3 specifies requirements for internal auditing.

9.1 PIV Card Revocation

PIV Cards and the corresponding certificates must be revoked if any of the following occurs:

- An employee separates (voluntarily or involuntarily) from Federal service;
- An employee separates from the Federal contractor;
- A contractor changes positions and no longer needs access to Federal buildings or systems;
- A cardholder reports a card as lost or compromised;
- Cardholder attributes included on the PIV card change (e.g., the cardholder ceases to act as a first responder);
- A cardholder is determined to hold a fraudulent identity; or
- An employee passes away.

These events may be difficult to detect. Procedures for PIV card revocation must be integrated into agency procedures to ensure effective card management. In addition, events within a contracting company may be obscured from an agency's view. Procedures for handling such events must be developed and included in contract language.

When these events are reported, normal operational procedures must be in place to ensure that:

- The PIV card itself is revoked. Local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status.
- The PIV Certificate Issuer is informed and certificates corresponding to asymmetric keys on the PIV card are revoked. CRLs are issued including the appropriate certificate serial numbers.
- OCSP Responders are updated so that queries with respect to certificates on the PIV card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the server's internal database.)
- Where possible, the PIV card shall be collected and destroyed. Where the card cannot be collected, normal operational procedures shall complete within 18 hours of notification.

In some cases, 18 hours is an unacceptable delay. For example, an agency may discover a cardholder's true identity is a person on a terrorist watch list. In such a case, emergency procedures must be executed to disseminate this information as rapidly as possible. Agencies are required to have procedures in place to update all servers in one hour in the case of such an emergency.

9.2 PIV Card Issuer Certification and Accreditation

OMB A-130 established government wide requirements for certification and accreditation (C&A) of federal computing systems. NIST has developed technical guidelines to assist agencies performing C&A. Specifically, FIPS 199 establishes security categories for information. NIST SP 800-37 and the draft FIPS 200 provide guidelines for C&A. As per OMB A-130, C&A must be performed every three years or whenever a major system change is implemented.

To ensure that systems are operated at a consistent level of assurance, this document establishes a baseline Security Categorization for the PIV Card Management System. Agencies may designate the PIV Card Management system information as FIPS 199 Medium or High for Integrity at their discretion. Agencies shall not designate these systems as FIPS 199 Low. These requirements do not constrain the security categorization for applications that rely on the PIV Card system.

C&A may be performed piecewise if the system is architected as separate components. For example, an agency may rely on a PKI vendor to manage certificates, but operate the card issuance in-house. While these systems are clearly related, an agency may perform C&A in two steps.

[COMMON] supplements the standard C&A requirements with a compliance audit for the PKI component of the PIV Card Management system. The compliance audit compares the certificate issuer's (e.g., the CA's and RA's) procedures and compares

them with the policies in [COMMON], then reviews operations to ensure personnel are implementing the documented procedures. The compliance audit must be performed yearly.

Additional related requirements are imposed by the Federal Information Security Management Act (FISMA). In particular, FISMA requires annual self assessment, which can include penetration testing. The "red team" concept should be employed by agencies to ensure that common vulnerabilities (e.g., unimplemented security patches) do not undermine the security of the PIV system.

9.3 Internal Auditing for PIV Card Management

C&A will detect systemic flaws in system architecture or implementation, but is not designed to detect particular events or failures. To detect issuance of fraudulent cards or other malfeasance by the personnel operating the PIV Card system, regular audit reviews shall be conducted by a trusted third party. The PIV system auditor may not hold any other operational role in the system.

ANNEX A: PIV CERTIFICATION AND ASSURANCE PROCESS

The PIV system is certified to be FIPS 201 compliant after each of its constituent components (Card, Reader, Issuer Software and Registration Database) has met its individual certification requirements. Since these individual certification requirements are based on different standards and it is a commercial reality that there is no single test laboratory that is accredited for certifying products built to all of these standards, a PIV system has to undergo testing and consequent certification through multiple certification facilities. The PIV components and their certification requirements are summarized in Table A-1:

Table A-1: PIV System Components & Certification Requirements

PIV Component	Certification Requirement (s)
1. PIV Card	(a) ISO/IEC 7816 (b) ISO/IEC 14443 (Parts 1-4) (c) Crypto Modules – FIPS 140-2
2. PIV Reader	(a) PC/SC
3. Card Issuance and Management System	(a) Crypto Modules – FIPS 140-2

A.1 Certification Facilities for FIPS 140-2 Testing

All of the cryptographic modules in the PIV system (both on-card and issuer software) shall be certified to be FIPS 140-2 Level 2 (or higher) compliant. The test facilities for FIPS 140-2 testing (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) are the nine Cryptographic Module Testing (CMT) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) program of the National Institute of Standards and Technology (NIST). Vendors wanting to supply cryptographic modules for the PIV system can select any of the nine accredited laboratories. The tests conducted by these laboratories for all vendor submissions are validated and a validation certificate for each vendor product is issued by the Cryptographic Module Validation Program (CMVP) – a joint program that is run by NIST and Communications Security Establishment (CSE), a Canadian government agency. The details of the CMVP, NVLAP programs and the list of CMT laboratories can be found in the CMVP website - http://csrc.ncsl.nist.gov/cryptval.

A.2 PIV System Assurance Process

Assurance that PIV systems are compliant with FIPS 201 shall be provided through a comprehensive accreditation and certification program (hereafter referred to as FIPS 201 Validation Program). FIPS 201 Validation program will differ from some of the other security validation programs in the U.S government in the following ways:

(a) Multiple Components: The FIPS 201 Validation program involves certification process for an entire system (as opposed to a single product or module) that consists of multiple components.
(b) Multiple Standards: Each of the PIV components may have to be certified for different standards.

The list of PIV components and the standards for which they must be certified are given in Table A-2 below:

Table A-2: PIV Components and Conforming Standard

PIV Component	Conforming Standard
1. PIV Card – Physical Characteristics, Communication Protocol & Signals	(a) ISO/IEC 7810 (b) ISO/IEC 7816 (c) ISO/IEC 14443
2. PIV Card – ON-card Crypto Modules & associated Algorithms	FIPS 140-2
3. PIV Reader	(a) PC/SC (b) ISOIEC 7816 (c) ISO/IEC 14443
4. Card Issuance and Management System	FIPS 140-2

A.2.1 Scope of FIPS 201 Validation Testing

The FIPS 201 Validation program will not involve testing for compliance to every one of the standards referred above. PIV components conforming to industry-wide standards are procured pre-certified. The following pre-certified PIV components will not be subject to unit tests under the FIPS 201 Validation program.

Table A-3: Standards for Pre-certified Components

Pre-Certified PIV Component	Associated Standard
1. PIV Card (without Crypto Modules)	ISO IEC 7816, ISO/IEC 14443
2. PIV Reader	PC/SC

The following PIV components shall be subject to testing under the FIPS 201 Validation Program. The rationale for choosing these components for direct testing is that they are either function modules involved in the core function of identity credential verification or service modules called from those function modules to perform specific functions (e.g., crypto-service modules performing functions like signing a message, verifying a message signature, retrieving a certificate etc).

Table A-4: Standards for Validated Components

FIPS 201 Validated PIV Component	Associated Standard
1. PIV Card –On-card Crypto Modules	FIPS 140-2
2. Card Issuance and Management System	FIPS 140-2

The FIPS 140-2 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) standard stipulates certain security requirements for cryptographic modules (both hardware and software) and classifies those requirements into four overall levels in the increasing order of stringency. The crypto module used in a PIV component (on-card or in issuer software) should at be certified for FIPS 140-2 Level 2 or higher.

Besides conformance to the established standards, FIPS 201 validation may involve some minor tests for conformance to the issuing agency's policies. One of them is the verification of the credentials in the PIV card for conformance to the issuing agency's privacy policy.

Since the FIPS 201 card is intended to provide, not only physical access, but also logical access to IT systems, a FIPS 201 card shall include modules that support access control/authorizations by a variety of information systems supported by issuing agencies. These modules, irrespective of whether they are resident in the PIV card or in the issuer software (client application), will not come directly under the scope of FIPS 201 validation testing. They will however come under the scope of the FIPS 201 validation maintenance measures described in section A.2.4.

A.2.2 Tasks for Setting Up the FIPS 201 Validation Program

The following tasks shall be undertaken by NIST to set up the FIPS 201 Validation Program.

(a) Accreditation of Testing Laboratories: Testing Laboratories involved in FIPS 201 testing will be accredited through the National Voluntary Laboratory Accreditation Program (NVLAP). Since there already exist laboratories (i.e., the nine Cryptographic Module Testing (CMT) laboratories) for FIPS 140-2 testing under this accreditation scheme, the main task will be to accredit laboratories for FIPS 201 testing.
(b) Guidance Documents: NIST shall develop guidance documents for various stakeholders. This shall include PIV component vendors who want to have their products validated for FIPS 201

A.2.3 Steps for Acquiring FIPS 201 Validation Certificate

(a) Vendors interested in having their products validated for FIPS 201 compliance may approach any of the FIPS 201 accredited laboratories for testing their PIV system modules.
(b) The testing laboratories shall perform the tests conforming to the relevant

standards specified in FIPS 201.

(c) The tests shall be validated and a certificate will be issued by the FIPS 201 Validation Program office for those modules that were tested.

A.2.4 Validation Maintenance

It is anticipated that there will be activities performed on one or more of the PIV system modules by the issuing agency after the procurement of a FIPS 201 validated system and issuance of PIV cards. Examples of these post-issuance activities include:

(a) New applications are loaded to the PIV card by another agency.
(b) Application modified for access to new information systems or changing access control mechanisms for existing PIV system.

These two types of post-issuance activities have different impacts on FIPS 201 validation. Whenever there is change in card issuance system and card design, the issuing agency shall re-certify the PIV card issuance system to ensure that privacy requirements of the credentials are still met. Whenever new modules are added to the card or the issuer software, re-certification shall be required in order to ensure that these new modules do not interfere with the crypto modules or affect the interoperability between the issuer software and the PIV card.

ANNEX B: PUBLIC KEY INFRASTRUCTURE FOR THE PIV CARD

PIV cards consistent with this specification may have one, two, or three asymmetric private keys. All PIV cards will include a *PIV authentication key*. PIV cards may also support a *digital signature key* and a *key management key*.

To manage the associated public keys, agencies are required to issue and manage X.509 public key certificates as specified below. PIV cards may store and re-distribute the X.509 certificate(s) associated with their private key(s). Certificate status is provided by both X.509 Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responders.

B.1 Policy

All certificates issued to support PIV card authentication shall be issued under the id-CommonHW policy and the id-CommonAuth policy[8] as defined in the *X.509 Certificate Policy for the Common Policy Framework* [COMMON]. These requirements cover identity proofing as well as the management of certification authorities (CAs) and registration authorities (RAs). CAs and RAs may be operated by agencies, or outsourced to PKI Service Providers. For a list of PKI Service Providers who have been approved to operate under [COMMON], see http://www.cio.gov/ficc/cpl.htm

[COMMON] requires FIPS 140-2 Level 2 validation for the subscriber cryptomodule (i.e., the PIV). In addition, this specification requires the cardholder to authenticate to the PIV card each time it performs a private key computation with the *digital signature key* or *key management key*.

[COMMON] imposes a minimum of RSA key length of 1024 bits for CA key sizes, and mandates use of SHA-1 and SHA-256 hash algorithms. CAs must use 2048 bit RSA keys when signing certificates and CRLs that expire on or after December 31, 2008. CAs that generate certificates and CRLs under this policy shall use SHA-1 or SHA-256 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued before January 1, 2007 shall be generated using SHA-1. Signatures on certificates and CRLs that are issued between January 1, 2007 and December 31, 2009 (inclusive) shall be generated using either SHA-1 or SHA-256. Signatures on certificates and CRLs that are issued on or after January 1, 2009 shall be generated using SHA-256.

Note that additional cryptographic algorithms (e.g., ECDSA) are specified in the following text. Future enhancements to [COMMON] are expected to permit use of additional algorithms. For conformance to this specification, PIV card management systems are limited to algorithms and key sizes recognized by this Annex and the current

[8] The id-CommonAuth policy has not yet been drafted. This policy will be used to differentiate simple authentication keys, where user interaction is not required, from signature keys where the operation is expected to demonstrate explicit user intent.

version of [COMMON].

B.2 Architecture

CAs that issue certificates to support PIV card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-Signed, Self-issued, and CA certificates issued by these CAs shall conform to *Worksheet 1: Self-Signed Certificate Profile, Worksheet 2: Self-Issued CA Certificate Profile,* and *Worksheet 3: Cross Certificate Profile* respectively in [PROF].

B.3 X.509 Certificate Contents

The required contents of X.509 certificates associated with PIV private keys are based on the X.509 Certificate and CRL Profile for the Common Policy [PROF]. The relationship is described below:

- HTTP URIs required by [PROF] in the SIA, AIA, and CDP extensions are optional for this specification;
- AIA extensions shall include pointers to the appropriate OCSP status responders, using the id-ad-ocsp access method as specified in Section 8 of [PROF], in addition to the LDAP URIs required by [PROF].
- If private key computations can be performed with the *PIV authentication key* without user intervention (beyond that required for cryptomodule activation), the corresponding certificate must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension.
- Certificates containing the public key associated with a digital signature private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF].
- Certificates containing the public key associated with a PIV authentication private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF], but shall not assert the nonRepudiation bit in the keyUsage extension and must include the PIV card's FASC-N in the subject alternative name field.
- Certificates containing the public key associated with a key management private key shall conform to *Worksheet 6: Key Management Certificate Profile* in [PROF].
- Requirements for algorithms and key sizes for each of the three types of PIV asymmetric keys are given in the table below.[9]

[9] The current text of [COMMON] permits only RSA with SHA-1 and SHA-256. Supporting DSA, Diffie-Hellman and elliptic curve algorithms will require a change in [COMMON].

Table B-1: PIV Private Key Type

PIV Private Key Type	Certificate Expiration Date	Algorithms & Key Sizes
PIV authentication key	Through 12/31/2010	RSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	RSA 2048 bits or higher; ECDSA 224 bits or higher
Digital signature key	Through 12/31/2007	RSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2007	RSA 2048 bits or higher; ECDSA 224 bits or higher
Key management key	Through 12/31/2007	RSA/D-H 1024 bits or higher; ECDH 160 bits or higher
	After 12/31/2007	RSA/D-H 2048 bits or higher; ECDH 224 bits or higher

B.4 X.509 CRL Contents

CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to *Worksheet 4: CRL Profile* in the X.509 Certificate and CRL Profile for the Common Policy [PROF].

B.5 Certificate and CRL Distribution

This specification requires distribution of CA certificates and CRLs using the Lightweight Directory Access Protocol (LDAP). Distribution of user certificates with LDAP is optional, but fully specified. Distribution of certificate status information using OCSP status responders is also required.

B.6 LDAP distribution

At a minimum, CA certificates and CRLs shall be distributed using LDAP. Specific requirements are found in *Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements* of the Shared Service Provider Repository Service Requirements [SSP REP].

It is an agency decision whether or not user certificates are distributed via LDAP. When user certificates are distributed, the requirements in *Table IV – End-Entity Certificate Repository Service Requirements* of [SSP REP] shall be satisfied.

B.7 OCSP Status Responders

OCSP status responders shall be implemented as a supplementary certificate status

mechanism. The OCSP status responders must be updated at least as frequently as CRLs are issued. The definitive OCSP responder for each certificate shall be specified in the AIA extension as described in [PROF].

B.8 Migration From Legacy PKIs

Agencies whose PKI has cross-certified with the Federal Bridge CA (FBCA) at Medium or High may continue to assert agency specific policy OIDs through December 31, 2007. Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Agencies may continue to assert agency specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008..)

ANNEX C PIV SUPPORT FOR ACCESS CONTROL MECHANISMS (INFORMATIVE)

FIPS 201 provides identity card-based support for both logical and physical access control systems.

C.1 Physical Security Support

The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group has drafted *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* (PACS). Table C-1 differentiates among low, moderate, and high PACS assurance profiles and lists PIV card features available to support the three profiles.

Table C-1: PIV Support For PACS

Assurance Level	Basic Requirement	PIV Card Support
PACS Low	Recognition of Unique Cardholder Identifier string (i.e., FASC-N) and matching to Access List	Unique Cardholder Identifier string (i.e., FASC-N)
PACS Medium	Use of Unique Cardholder Identifier string (i.e., FASC-N) and Card Unique Identifier (i.e., CUID) to derive unique authentication string and matching to access list.	Unique Cardholder Identifier string (i.e., FASC-N) and Card Unique Identifier (i.e., CUID). Digitally Signed Unique Card Identifier and Expiration Date[10]
PACS High	Cryptographic Challenge/Response Protocol	PIN Capture/Storage and Cryptographic Engine and Key Management Support
Other Support Features	-	Signed Digital Biometric Information That Can Be Used In Matching of Biometric Information Stored on Card to Biometric Information Captured By Access Control Mechanisms

[10] The PIV standard extends the standard CHUID data structure to add a Expiration Date element as described in Section 6.4.2.

C.2 Logical Access Support

For logical access control, FIPS 201 incorporates by reference NIST Special Publication 800-63 (SP 800-63), *Electronic Authentication Guideline*. SP 800-63 supplements OMB guidance, *E-Authentication Guidance for Federal Agencies* (OMB 04-04) that defines four levels of authentication Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance, and Level 4 is the highest. Table C-2 summarizes electronic authentication requirements and PIV support to electronic authentication functions.

Table C-2: PIV Support For E-Authentication

Assurance Level	Basic Requirement	PIV Card Support
1	Password-based Access Control	
2	Access control Based on "Strong Passwords"	
3	Proof of Possession of a Key or a One-time Password Through a Cryptographic Protocol.	Cryptographic Mechanisms Including Signed Key Certificate (May use "soft" Card or one-time password device)
4	-	Cryptographic Mechanisms Including Signed Key Certificate (Must use "hard" Card)

ANNEX D: REFERENCES

[ANSI322] ANSI INCITS 322, Card Durability Test Methods

[CBEFF] NISTIR 6529-A - Common Biometric Exchange Formats Framework (CBEFF)

[COMMON] X.509 Certificate Policy for the Common Policy Framework, February 10, 2004. Available at http://www.cio.gov/ficc/documents/CommonPolicy.pdf

[FIBIF] ANSI/INCITS 381-2004 - Finger Image Based Interchange Format

[FFSMT] ANSI/NIST-ITL 1-2000 – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information

[EFTS/F] Appendix F of the FBI's Electronic Fingerprint Transmission Specification (EFTS/F)

[FLATS] NISTIR 7110 - C. L. Wilson, M. D. Garris, and C. I. Watson, Matching Performance for the USVISIT IDENT System Using Flat Fingerprints, National Institute of Standards and Technology, (May 2004).

[FRFD] ANSI/INCITS 385-2004 - Face Recognition Format for Data

[G90-98] ASTM G90-98

[G155-00] ASTM G155-00

[INCITS/M1-040211] ANSI/INCITS M1-040211 – Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers

[IR7116] NISTIR 7116

[ISO14443] ISO/IEC 14443-1:2000 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards, 2000-04-15

[ISO373] ISO/IEC 10373

[ISO7810] ISO/IEC 7810:2003 Identification Cards – Physical Characteristics, 2003-11-01

[ISO7816] ISO/IEC 7816 Identification Cards – Integrated Circuits with Contacts http://www.iso.ch.

[MINEX04] - http://fingerprint.nist.gov/minex04/index.html

[NIST91] NIST Publications List 91 – Computer Security Publications

[NFIQUA] NISTIR 7151 – NIST Fingerprint Image Quality (NFIQ)

[OMB130] Office of Management and Budget, OMB A-130

[OMBx04] Office of Management and Budget, OMB 04-04

[PACS] PACS v2.2 – The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2 July 27, 2004.

[PCSC] – Personal Computer/Smart Card Workgroup Specifications, http://www.pcscworkgroup.com.

[PROF] X.509 Certificate and CRL Profile for the Common Policy, Version 1.1 July 8, 2004. Available at http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf

[SP8x30] NIST Special Publication 800-30

[SP8x37] NIST Special Publication 800-37

[SP8x53] NIST Special Publication 800-53

[SP800-63] Appendix A in NIST SP 800-63, *Electronic Authentication Guideline*.

[SP800-xx] Integrated Circuit Card for Personal Identity Verification, Version 0.1, 2004-10-19

[SSP REP] Shared Service Provider Repository Service Requirements, January 23, 2004. Available at http://www.cio.gov/ficc/documents/SSPrepositoryRqmts.pdf

[VEND1] NIST IR 6965 - P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and M. Bone, 'Face recognition vendor test 2002, National Institute of Standards & Technology, Gaithersburg Maryland, March 2003.

[VEND2] NISTIR 7123 - C.L. Wilson, R. Austin Hicklin, Harold Korves, Bradford Ulery, Melissa Zoepfl, Mike Bone, Patrick Grother, Ross Micheals. Steve Otto and, Craig Watson, Fingerprint vendor technology evaluation 2003: summary of results and analysis report, National Institute of Standards and Technology, (June 2004).